PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/46

A2

(11) International Publication Number: WO 98/05146

(43) International Publication Date: 5 February 1998 (05.02.98)

(21) International Application Number: PCT/IL97/00258

(22) International Filing Date: 29 July 1997 (29.07.97)

(30) Priority Data:
118984 30 July 1996 (30.07.96) IL

(71) Applicant: MADGE NETWORKS (ISRAEL) LTD. [IL/IL]; Building 3, Atidim Technology Park, 61131 Tel Aviv (IL).

(72) Inventors: BERLOVITCH, Albert; Benyamin Fine Street 4, 75237 Rishon le Zion (IL). SHURMAN, Michael; Greenspan Street 4221, 93806 Jerusalem (IL). SHOUA, Menachem; Hapodim Street 30, 52574 Ramat Gan (IL).

(74) Agents: COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

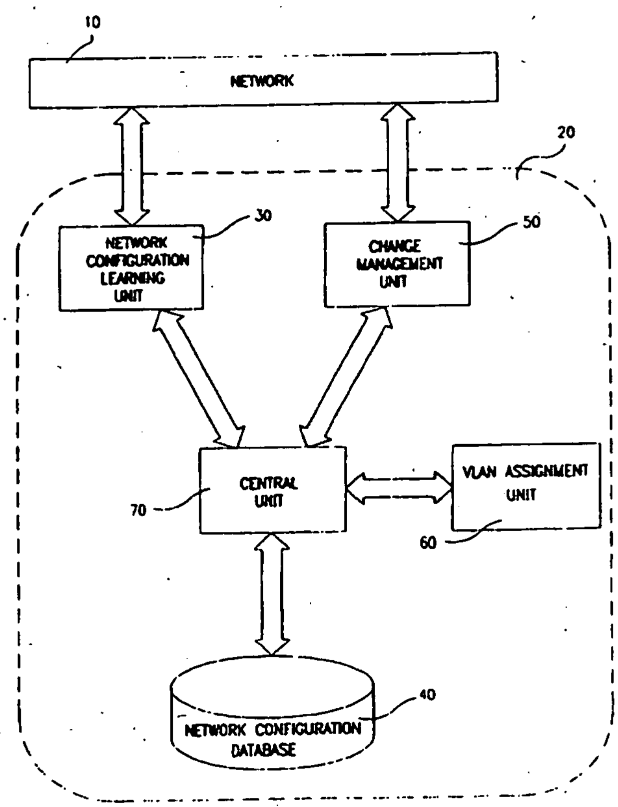
(81) Designated States: CN, JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: APPARATUS AND METHOD FOR ASSIGNING VIRTUAL LANs

(57) Abstract

This invention discloses an apparatus (20) for managing a switched routed network (10) including a network configuration learning unit (30) operative to learn a configuration of the switched routed network, a VLAN assignment unit (60) for generating a division of the network into virtual LANs (VLANs) based on the learn configuration of the network, and a change manager (50) operative to detect a change in the configuration of the network and to modify the division of the network into VLANs. A method for generating a division of a switched routed network into virtual LANs (VLANs) based on a learn configuration of the network is also disclosed.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

APPARATUS & METHOD FOR ASSIGNING VIRTUAL LANS

The present invention relates to apparatus and methods for network management.

ATMman Virtual LAN software, by Agile Networks, Ltd., is intended to inspect LAN traffic at the network layer and to create layer-3 based virtual LANs. Two key features are termed the Global Endstation Identification feature and the IP address management feature. Agile has stated that its end-station identification system allows the physical location and MAC address of each end-station on the network, as well as its protocol types, network-layer addresses, network-layer names and network function. The IP Address Management system is to maintain a database of layer 1, 2 and 3 information about each end-station on the network and informs administrators of any new, changed or duplicate IP addresses that appear.

The disclosures of all publications mentioned in the specification and of the publications cited therein are hereby incorporated by reference.

The present invention seeks to provide an improved method and apparatus for managing networks, including methods and apparatus which include any of the features described herein either individually or in any combination.

There is thus provided, in accordance with a preferred embodiment of the present invention, apparatus for managing a switched routed network including a network configuration learning unit operative to learn a configuration of the switched routed network, a VLAN assignment unit for generating a division of the network into virtual LANs (VLANs) based on the learned configuration of the network, and a change manager operative to detect a change in the configuration of the network and to modify the division of the network into VLANs.

Further in accordance with a preferred embodiment of the present invention, the configuration of the network includes physical configuration aspects and logical configuration aspects.

Also provided, in accordance with a preferred embodiment of the present invention, is apparatus for learning the configuration of a switched routed network, the network including a switching skeleton including at least one switching hub interconnected by a switch backbone, each switching hub including at least one port, and a plurality of end-stations each having a unique physical address and each communicating with an individual one of the switching hubs via one of the switching hub's ports, thereby defining a plurality of end-station to port connections, the plurality of end-stations including at least one router, the apparatus including an end-station to port connection

learning unit operative to learn associations between ports and physical addresses of the end-stations communicating therewith, a physical address - logical address association learning unit operative to learn associations between logical addresses and physical addresses, and an end-station to logical address association learning unit operative to derive associations between ports and logical addresses from the learned associations between ports and physical addresses of the end stations and the learned associations between logical addresses and physical addresses.

Further in accordance with a preferred embodiment of the present invention, the physical address-logical address association learning unit is operative to scan physical addresses of at least some of the plurality of end stations, and actively find an associated logical address upon encountering each physical address.

Further in accordance with a preferred embodiment of the present invention, each logical address includes an IP network layer address and wherein the network includes an IP network which is partitioned into a multiplicity of IP subnets and wherein each IP network layer address belongs to an individual one of the multiplicity of subnets and wherein the apparatus for learning also includes apparatus for determining all IP subnets into which the IP network is partitioned.

Still further in accordance with a preferred embodiment of the present invention, each logical address includes an IPX protocol network layer address and wherein the network is partitioned into a multiplicity of IPX networks and wherein each IPX protocol network layer address belongs to an individual one of the multiplicity of IPX networks and wherein the apparatus for learning also includes apparatus for determining all IPX networks into which the IPX network is partitioned.

Additionally in accordance with a preferred embodiment of the present invention, the physical address-logical address association learning unit is operative to send a multiplicity of ICMP echo request packets to each of at least some of the plurality of end stations, each echo request packet including a physical destination address and an IP network layer destination address which includes an IP broadcast address of an individual one of the multiplicity of subnets, and the echo request packet sent to an individual end station has a physical destination address which is the physical address of the individual end station.

Further in accordance with a preferred embodiment of the present invention, the physical address -logical address association learning unit includes an ICMP echo reply packet analyzer operative to derive a physical address - IP address association from each arriving ICMP echo reply packet.

Still further in accordance with a preferred embodiment of the present invention, the physical address-logical address association learning unit is operative to send an IPX

diagnostic packet to each of at least some of the plurality of end stations, an IPX diagnostic packet including a physical destination address and an IPX network layer destination address which includes an IPX broadcast address, and the IPX diagnostic packet sent to an individual end station includes an IPX diagnostic packet whose physical destination address is the physical address of the individual end station.

Additionally in accordance with a preferred embodiment of the present invention, the physical address -logical address association learning unit includes an IPX diagnostic packet analyzer operative to derive a physical address - IPX address association from each arriving IPX diagnostic reply packet.

Further in accordance with a preferred embodiment of the present invention, the physical address-logical address association learning unit includes an IP network layer address identifier operative, for each physical address, to passively identify a logical address including an IP network layer address, and the IP network layer address identifier is operative to listen for ARP packets and to analyze the ARP packets and derive therefrom IP network layer addresses.

Further in accordance with a preferred embodiment of the present invention, the network includes a NetWare network, (NetWare is commercially available from Novell Inc. of 122 East 1700 South, Provo, Utah 84606, USA), the plurality of end-stations includes at least one NetWare file servers and at least one NetWare clients, each of the NetWare clients is served by one of the at least one NetWare file servers, and the apparatus for learning also includes a server-client learner operative to identify servers and clients from among the plurality of end-stations and to learn relationships between the servers and the clients.

Also provided, in accordance with another preferred embodiment of the present invention, is a method for generating a division of a switched routed network into virtual LANs (VLANs) based on a learned configuration of the network, the network including a switching skeleton including at least one switching hubs interconnected by a switch backbone, each switching hub including at least one port, and a plurality of end - stations each having a unique physical address and each communicating with an individual one of the switching hubs via one of the switching hub's ports, thereby defining a plurality of end-station to port connections, the plurality of end-stations including at least one router, the method including dividing the plurality of end-stations into nodes, wherein each node includes a set of at least one end-station, connecting each first and second node from among the nodes with an arc if at least one of the end-stations in the first node set is associated with the same port as at least one of the end-stations in the second node set, thereby to generate at least one disjoint graphs, and allocating a VLAN to each of the at least one disjoint graphs characterized in that packets sent by an

individual end-station connected to a port belonging to an individual VLAN, including broadcast packets, are transmitted only to end-stations connected to one of the ports within the same VLAN.

Further in accordance with a preferred embodiment of the present invention, the network includes an IP network which is partitioned into a multiplicity of IP subnets and the sets respectively correspond to the IP subnets.

Still further in accordance with a preferred embodiment of the present invention, the network is partitioned into a multiplicity of IPX networks and the sets respectively correspond to the IPX networks.

Additionally in accordance with a preferred embodiment of the present invention, the network includes a NetWare network and wherein the plurality of end-stations includes at least one NetWare file servers and at least one NetWare clients and wherein each of the NetWare clients is served by one of the at least one NetWare file servers, and wherein each of the sets includes an individual NetWare file server and the NetWare clients served thereby.

Still further in accordance with a preferred embodiment of the present invention, the VLANs are allocated so as to increase the number of clients which communicate directly with their servers rather than via a router.

Further in accordance with a preferred embodiment of the present invention, the method also includes the step of allocating global VLANs to at least one of the ports so as to reduce the number of end-station pairs which hear broadcast packets arriving to one another.

Still further in accordance with a preferred embodiment of the present invention, the method also includes the step of allocating global VLANs to at least one of the ports so as to minimize the number of end-station pairs which hear broadcast packets arriving to one another.

Also provided, in accordance with another preferred embodiment of the present invention, is a method for detecting a change in the configuration of a switched routed network, the network including a plurality of network elements, and for modifying a division of the network into VLANS, the method including detecting at least one event at an individual network element including detecting the identity of the individual end-station, the event including at least one of the following: at least one logical change, at least one physical change, and at least one communication failure, and categorizing at least one event as a problematic event or a non-problematic event and, if the event is categorized as problematic, alleviating the failure situation.

Further in accordance with a preferred embodiment of the present invention, the at least one physical change includes at least one of the following: at least one new end-

station added at at least one individual port within the network, and at least one end-station which has moved from a first port within the network to a second port within the network.

Still further in accordance with a preferred embodiment of the present invention, at least one logical change includes an IP address of at least one end-station which has changed.

Additionally in accordance with a preferred embodiment of the present invention, at least one communication failure includes at least one of a failed attempt of a NetWare client end-station to initially connect to a server end-station, and a NetWare client end-station which has been disconnected from a server end-station.

Further in accordance with a preferred embodiment of the present invention, the analyzing and alleviating step includes detecting a mismatch between the network address of an end-station and a VLAN to which the port to which the end-station is connected belongs, determining a new VLAN which matches the network addresses of all end-stations connected to the port, and assigning the new VLAN to the port.

Also provided, in accordance with another preferred embodiment of the present invention, is apparatus for generating a VLAN assignment scheme according to which individual components of a network are assigned to VLANs, the apparatus including a reserved port designator operative to accept a user's designation of ports within the network to which no VLAN is to be assigned, and a VLAN assignment scheme generator operative to generate a VLAN assignment scheme according to which only components of the network other than the reserved ports are assigned to VLANs.

Also provided, in accordance with yet another preferred embodiment of the present invention, is apparatus for managing a switched routed network including a network configuration learning unit operative to learn a configuration of a switched routed network including an existing division into VLANs, and a VLAN assignment unit for generating a new division of the network into virtual LANs (VLANs) based on the learned configuration of the network, wherein the network configuration learning unit includes a diagnostic unit for analyzing and diagnosing the existing division of the network into VLANs.

Further in accordance with a preferred embodiment of the present invention, the diagnostic unit is operative to identify end-stations which belong to the same IP subnet and which are connected to ports assigned to different VLANs.

Still further in accordance with a preferred embodiment of the present invention, the diagnostic unit is operative to identify Novell servers belonging to different IPX networks which are connected to ports assigned to a single VLAN.

Additionally in accordance with a preferred embodiment of the present

invention, the diagnostic unit is operative to identify IPX routers belonging to different IPX networks which are connected to ports assigned to a single VLAN.

Further in accordance with a preferred embodiment of the present invention, the method also includes storing a record of problematic and non-problematic events occurring at network elements.

Still further in accordance with a preferred embodiment of the present invention, the record of problematic events includes, for each problematic event, a description of a contradictory VLAN assignment associated with the problematic event.

Further in accordance with a preferred embodiment of the present invention, the record of problematic events includes, for at least one problematic event, a recommendation describing how a human operator may resolve the contradictory VLAN assignment.

Additionally in accordance with a preferred embodiment of the present invention, the record of problematic events includes, for at least one problematic event, a description of a system action which resolves the contradictory VLAN assignment.

Further in accordance with a preferred embodiment of the present invention, the step of alleviating includes alerting a human operator that a problematic event has occurred.

The methods and apparatus of the present invention herein collects data pertaining to the IP or IPX configuration of the network. This data is employed by a rule-based system, typically implemented in software, which applies predefined rules to assign virtual LANs to the network, so as to conform as closely as possible to predetermined bestness criteria. It is appreciated that some or all of the particular rules and criteria employed are application-specific. Specifically, the specific implementation of a virtual LAN in the hardware may affect the rules and/or criteria. If, for example, the hardware implements a global LAN, then the rule-based system may be based on improving or optimizing a broadcast matrix whereas the rule-based system may not be based on this criterion if the hardware does not implement a global LAN.

According to a preferred embodiment of the present invention, the elements of a network are grouped into predefined entities such as sets or graphs. The apparatus and methods of the present invention are based on computational processes which operate on these predefined entities. The rules and criteria for grouping may be application-specific, however, the computational processes are preferably defined generally enough so as to be operational in conjunction with different application-specific rules and criteria.

The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified block diagram of apparatus for managing a network

constructed and operative in accordance with a preferred embodiment of the present invention,

Figs. 2A - 2E are simplified flowchart illustrations of 5 subprocesses which, when performed simultaneously or in parallel, together define a preferred mode of operation for the network configuration learning unit of Fig. 1,

Fig. 3 is a simplified flowchart illustration of a preferred mode of operation for the change manager of Fig. 1,

Fig. 4 is a simplified flowchart illustration of a preferred mode of operation for the VLAN assignment unit of Fig. 1,

Fig. 5 is a simplified block diagram illustration of a network and an end-station on which software apparatus for managing the network may be run, the diagram also including VLAN assignment information generated by the software apparatus,

Fig. 6 is a simplified block diagram illustration of a VLAN assignment generated by the software apparatus shown and described herein, for a Novell network,

Fig. 7 is a simplified block diagram illustration of a VLAN assignment generated by the software apparatus shown and described herein, for a Novell network portion in which clients of different servers are connected to the same port,

Fig. 8 is a simplified block diagram illustration of a VLAN assignment generated by the software apparatus shown and described herein, for a more complex Novell network portion including servers with IPXNs between which there is no routing path,

Fig. 9 is a simplified block diagram illustration of a VLAN assignment generated by the software apparatus shown and described herein, for a Novell network portion including a port to which both an end-station and a server are connected,

Fig. 10 is a simplified flowchart illustration of a preferred mode of operation for the "build port to network association list table" block of Fig. 4,

Fig. 11 is a simplified flowchart illustration of a preferred mode of operation for the "build network representation graph" block of Fig. 4,

Fig. 12 is a simplified flowchart illustration of a preferred mode of operation for the "find best cut in network representation graph" block of Fig. 4,

Fig. 13 is a screen generated by a software embodiment of the present invention for a network including 4 IP subnets and 3 IPX networks,

Fig. 14 is a pictorial illustration of a screen generated by a VLAN assigning system which prompts a user to define reserved ports to which no VLAN is to be assigned,

Fig. 15 is a simplified flowchart illustration of a preferred method of operation for VLAN assignment apparatus constructed according to a preferred embodiment of the present invention and operative to identify contradictions in an existing VLAN

assignment, and

Fig. 16 is a pictorial illustration of a screen which includes a warning regarding a problematic event and an indication of a non-problematic event.

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

Fig. 1 is a simplified block diagram of a network 10 and apparatus 20 for managing a network constructed and operative in accordance with a preferred embodiment of the present invention. The network typically comprises a switching skeleton including at least one switching hubs interconnected by a switch backbone, each switching hub including at least one port and a plurality of end-stations each having a unique physical address and each communicating with an individual one of the switching hubs via one of the switching hub's ports, thereby defining a plurality of end-station to port connections, the plurality of end-stations including at least one router.

The apparatus 20 of Fig. 1 includes a network configuration learning unit 30 which is operative to learn the configuration of the network 10 and store information defining the configuration in a network configuration database 40. A preferred method of operation for unit 30 is described below with reference to Figs. 2A - 2E.

The apparatus 20 also includes a change management unit 50 and a VLAN assignment unit 60. The change management unit 50 is operative to monitor changes in the configuration of the network 10, and to change the configuration-defining information in database 40 accordingly. The change management unit 50 is described in detail below with reference to Fig. 3. The VLAN assignment unit 60 is operative to assign individual components of a switched routed network into virtual LANs (VLANs) based on a learned configuration of the network.

A virtual LAN (VLAN) is a broadcast domain, i.e. a plurality of end-stations interconnected by one or more switches such that the end-stations can communicate as though they were connected by a single physical broadcast LAN. Typically, a VLAN is a set of ports characterized in that packets sent by an individual end-station connected to a port belonging to the individual VLAN can be transmitted to end-stations connected to a port which is not within the same VLAN, only via a router.

The operation of VLAN assignment unit 60 is described in detail below with reference to Fig. 4. Generally speaking, the method comprises:

a. dividing the plurality of end-stations of the network 10 into nodes, wherein each node comprises a set of at least one end-station;

b. connecting each first and second node from among the nodes with an arc if at least one of the end-stations in the first node set is associated with the same port as at least one of the end-stations in the second node set, thereby to generate at least one disconnected graphs;

c. allocating a VLAN to each of the at least one disjoint graphs characterized in that broadcast packets sent by an individual end-station connected to a port belonging to an individual VLAN are transmitted only to end-stations connected to one of the ports within the same VLAN.

Reference is now made to Figs. 2A - 2E which are simplified flowchart illustrations of 7 subprocesses which, when performed simultaneously or in parallel, together define a preferred mode of operation for the network configuration learning unit of Fig. 1. Each of the subprocesses of Figs. 2A - 2E is preferably defined as an object within the network configuration learning unit 30 of Fig. 1.

Fig. 3 is a simplified self-explanatory flowchart illustration of a preferred mode of operation for the change manager 50 of Fig. 1.

Fig. 4 is a simplified self-explanatory top-level flowchart illustration of a preferred mode of operation for the VLAN assignment unit 60 of Fig. 1. Figs. 10 - 12 are simplified self-explanatory flowchart illustrations of preferred modes of operation for the "build port to network association list table", "build network representation graph" and "find best cut in network representation graph" blocks, respectively, of Fig. 4.

A detailed description of a network managing system which assigns each component of a network to VLANs, as described above, is now provided.

0.1. Scope

This section describes the specifications of Virtual Network Server - an application intended to perform automatic Virtual LAN configuration in IP and Novell networks. Besides general function of the application and implementation specification, the section describes different cases of network configuration, explains networking software behavior and defines a set of rules for Virtual LAN assignment, especially for Novell network.

0.2. Abbreviations

The following abbreviations will be used in this section.

VLAN	- Virtual LAN
VNS	- Virtual Network Server
IPSN	- IP Subnetwork

IPX	- Internal Packet eXchange
IPXN	- IPX Network
SAP	- Server Advertisement Protocol
RIP	- Routing Information Protocol
NCP	- NetWare Core Protocol
ARP	- Address Resolution Protocol
RARP	- Reverse Address Resolution Protocol
DB	- Database
MAC	- Media Access Control
IP	- Internet Protocol
RIP	- Routing Information Protocol
CAM	- Content Addressable Memory
ICMP	- Internet Control Message Protocol
DM	- Device Manager, as described in the user-manual of the MultiMan application, commercially available from Madge
NIC	- Network Interface Card
SNMP	- Simple Network Management Protocol

C1, C2, S1, S2 etc. are examples of Novell end-stations, where C means client and S means server.

Management Platform is a commercial network management application that provides general network management services. An example of Management Platform is HP/OpenView (HP/OV) commercially available from Hewlett-Packard.

Madge applications such as TerrainMaster, VNS, etc. are integrated into HP/OV.

0.3. Overview

Virtual LAN has become a powerful facility for logical network division implemented on the physical layer. The main problem for the network manager who wants to use VLANs, is the hard work of VLAN configuration. The network manager may perform the VLAN assignment manually for all LANSwitch ports to which the stations are connected. This work may be done in two phases: first on network initialization (a one-time process but very hard) and second on a station logical address or physical connection change that is difficult to follow and during which is difficult to

reassign the VLAN without destroying previously defined configuration.

Virtual Network Server comes to perform automatic VLAN configuration in a switch/routing environment. The main goal of this configuration is to achieve compliance with existing logical network division on Layer 3 of OSI model. The optimal solution would be to configure the VLANs for all Layer 3 protocols. The first VNS release is implemented for IP and Novell networks only.

As the network manager's work on VLAN configuration is done in two phases, the VNS also performs its work in two phases: initialization and change management. In initialization phase, the VNS scans the network and builds a table that maps IP Subnets/Novell servers and their clients to the VLAN. According to this table, VLAN assignment is performed to relevant LANSwitch ports. Then the VNS listens for changes such as station moves, station IP address changes, Novell servers IPX Net changes, etc. and reassigns the VLAN to the port at which the change occurred.

The VNS obtains necessary information from the management platform, from DM and from Novell servers directly. The change management is performed by listening for broadcasts transmitted by the stations that lost connection and for traps sent by management agents on changes which occurred in the LANSwitch port.

1. Agent

In order to provide fast CAM polling and efficient change management, the following feature of the agent software is implemented. The agent receives from the sensor of the LANSwitch card the trap which indicates CAM content change. (The trap sending is already implemented in the sensor software of all released LANSwitch modules) When this trap is received, the agent updates the value of the MIB variable lseIntPortCAMLastChange by current sysUpTime and send configuration change trap to the console. The exact MIB variable definition and trap format are described in 2.1 and 2.2.

The CAM change indication is implemented in the network management agent.

2. MIB Support

2.1. Madge MIB

The MIB variable lseIntPortCAMLastChange is used by Madge MIB for VNS support. It indicates CAM content change. This variable has TimeTicks type and contains the value of sysUpTime for the moment the CAM content change is detected.

2.1.1. MIB Summary

The following table summarizes the new Madge MIB item used by the VNS application.

#	MIB item	Notes	Type
1	lseIntPortCAMLastChange	The value of sysUpTime at the time of CAM change detection	TimeTicks

2.2. Traps

When the value of lseIntPortCAMLastChange is changed, the agent sends the configuration change trap, containing this MIB variable. The following is a preferred format of the trap.

```
lseIntPortCAMLastChange TRAP-TYPE
        ENTERPRISE        IntBoxIdent
        VARIABLES {
                lseIntPortCAMLastChange
                }
        DESCRIPTION
                " This trap reports of the occurred configuration changes.
                It is enabled/disabled by chLntAgConfigChangeTraps."
        ::= 1
```

3. Console

3.1. General Principle of VLAN Assignment

As mentioned in the Overview, the main goal of the VNS is to achieve compliance between the logical network division on Layer 3 and the Virtual Networks. Therefore, the general principle of VLAN assignment is:

Logical Subnetwork = VLAN

For an IP network, this means that the stations belonging to the same IP subnet may get the same VLAN assignment. The optimal VLAN configuration for an IP network is to put each IP subnet on its own VLAN. However, it may happen that several IP subnets are on the same VLAN.

For a Novell environment, this means that a Novell server and the clients logged into it may get the same VLAN. In real life, the rules that the VNS respects are based on but not identical to the general principle of VLAN assignment.

3.2. VNS Station Configuration and Function Example

The VNS may get packets transmitted by the stations that reside on different VLANs. It may have the possibility to talk directly to these stations (not via the router). Therefore, it may be connected to the port configured on the Global LAN.

In order to provide direct dialog between the VNS and IP stations on an IP layer and over it, an IP source address of the packets sent by the VNS may belong to the IP Subnet of the destination station. That is to say, we may support multiple IP addresses for one Ethernet interface of a VNS station. Due to the requirement that an IP address may be unique for the network, the user may manually define the IP addresses for each IP subnetwork (IPSN) defined in the network.

For Novell processing, the VNS acquires information from the servers and IPX routers. Server connections are acquired directly from the server. Therefore, no special setting of the VNS station is needed for Novell processing and the only requirement is a global VLAN assignment.

Fig. 5 represents the VNS configuration and the result of its work in a mixed IP/Novell network.

In this example, there are three IPSNs and two IPXNs divided by the router.

Server S1 is configured on IPXN1 and has two clients: C1 and C2.

Server S2 is configured on IPXN2 and has one client C3.

The VNS supports three IP addresses on its interface which is connected to the port on Global Network. The result of VNS work is VLAN1 assignment to the stations and to the router interface that belongs to IPSN1, VLAN2 to IPSN2, VLAN3 to IPSN3, VLAN4 to IPXN1 and VLAN5 to IPXN2.

3.3. Operational Modes

As mentioned in the Overview, the VNS functions in two phases: initialization and change management.

There are two operational modes of the initialization phase:

1. Net to VLAN learning
2. Net to VLAN optimal proposition

In the Net2VN learning mode, the VNS acquires the current VLAN assignment of the LANSwitch ports. IP and Novell stations are connected to these ports and build a Net2VN mapping table according to the acquired information.

In the Net2VN proposition mode, the VNS builds the optimal Net2VN mapping table according to the methods described below. The proposition mode is the default mode of initialization.

A Net2VN table is displayed to the network manager who can modify it. Afterwards, the user may activate the VLAN's assignment. The VNS saves the table in a file, also termed herein the /usr/mmov/Save/vns.map file and perform the VLAN's assignment accordingly.

After initialization, the VNS automatically passes into the change management phase. There are two operational modes in this phase:

1. Automatic change
2. Confirmed change

In the automatic change mode, the VNS performs the VLAN reassignment without the user's intervention.

In the confirmed change mode, the VNS displays the pop-up window showing to the user the expected changes associated respectively with confirmation and cancellation. The VLAN assignment is performed only after user's confirmation. The confirmed change mode is the default mode of change management.

The user is able to modify the Net2VN table and to restart initialization at any moment.

UI is provided for changing the operational modes and for Net2VN table modification.

3.4. Interaction with User

The VNS is implemented as an automatic system, doing its job "silently", almost without the user's intervention. Nevertheless, there are some actions that the user can perform in order to refine the VNS and to follow up on errors and actions resulting from the VNS. The User Interface of the VNS provides the following features: initialization activation, Net to VLAN table confirmation and change, definition of reserved LANSwitch ports, backbone ports list, pop-up window for information and error

messages and confirmation window for VLAN assignment confirmation or cancel.

3.5. Managing LANSwitch Parameters

The basis of VNS work is LANSwitch configuration learning and managing. The VNS polls and gets updates on the set of configuration parameters and stores them in its database.

The station connection information is obtained from CAM content. The station is considered to be connected to some LANSwitch port if its MAC is detected in the CAM of this port. It may be that in most cases each MAC is detected in the CAM of only one LANSwitch port. If any one MAC is detected in the CAM of more than one port, the VNS performs CAM reset for these ports in order to get unique MAC appearance only in the right port.

A VLAN is assigned to a LANSwitch port by performing an SNMP Set of the following MIB variables: (lseIntPortRoutingMode to "Network Routing") **and** (genIntPortBusConnNumber to VLAN number or lseIntPortGlobalMode to "On" for global VLAN). Even if a successful SNMP Response is received, the VNS may verify that the Set has really succeeded. If the Set did not succeed, the VNS repeats it. This procedure is repeated three times. If it fails after the fourth time, the VNS informs the user.

As it was already mentioned, the LANSwitch port to which the VNS is connected, must be in Global mode. If it is not, the VNS configures it so that it is. If, during the work, the VNS detects that the Global mode of its port is switched off, it tries to fix this. If it fails, the user is informed and the VNS stops its work.

The following table summarizes the MIB variables that may be acquired and how the VNS uses of them.

MIB Variable	**Usage**
genGroupAutoManual	Determine, if the VLAN assignment is possible
lseGroupBackbone12	If the value is "On", do not learn the CAM of ports 1 and 2
lseGroupBackbone34	If the value is "On", do not learn the CAM of ports 3 and 4
genIntPortAdminStatus	Determine, if LANSwitch Port is active
genIntPortBusConnNumber	Get and set the VLAN number
lseIntPortRoutingMode	Get and set the VLAN (set value "Network Routing")
lseIntPortGlobal	Get and configure the port on the global VLAN (set value "On")

lseIntPortIOMode	If the value is "On", do not learn the CAM of the port
lseIntPortMACAddTable	Get CAM content, i.e. MAC addresses of connected stations
lseIntPortCAMLastChange	Get indication of CAM content change

3.6. IP Network

3.6.1. General Functions

The VNS identifies and polls the LANSwitch modules and the ports configuration, including CAM content (i.e. MAC addresses of connected stations). This information is obtained from management agents and stored in a VNS database. For each MAC detected in the CAM, the VNS tries to get a corresponding IP address from the management platform. If the management platform does not recognize the device, the VNS uses its special MAC to IP address resolution procedure to get the IP address (see 3.6.2). Then the IPSNs are taken from management platform. Using this information, the VNS activates a procedure that builds a table mapping all IPSNs to vlans (see 3.6.3). This table is displayed to user who can confirm or modify it. Afterwards, the vlans are assigned to all relevant LANSwitch ports according to the table.

The VNS detects new stations, moved stations and stations whose IP address was changed via the CAM change trap sent by the management agent and by listening for frequent ARP requests sent by stations which are unable to connect. The VNS reassigns the VLAN to the station's port according the above-mentioned table. If the new VLAN assignment contradicts an old one in that there are other stations connected to the same port, the assignment is performed as described in 3.6.4 (change management)

3.6.2. MAC to IP address resolution

The basis of VNS knowledge about the stations (i.e. MAC addresses of the stations) in the network is the content of the LANSwitch CAM connected to the LANSwitch ports. In order to acquire the IP addresses for LANSwitch port, the VNS may get an IP address for each MAC address. This function is especially critical for change management when the operation of acquiring an IP address for a MAC may be fast (couple of seconds).

The VNS uses its own method to solve the problem. For each IPSN, a special ICMP packet is sent with destination Ethernet address equal to the MAC address, whose IP we are looking for. The destination IP address is the IP broadcast address of the IPSN we are dealing with. The source IP address is the VNS IP address on this IPSN.

Generally, all the IP stations in the subnet reply to an IP broadcast because in standard implementation, it is sent to the Ethernet broadcast address, i.e. FF:FF:FF:FF:FF:FF. In our case, only necessary stations reply because the packet is sent to them as a unicast and the VNS obtains its IP address from the IP header of reply.

3.6.3. Initialization Phase in IP Network

Now, using the procedures defined above, we can specify the initialization procedure.

1. Identify and poll the management agents for the LANSwitch CAM, updating the VNS database.
2. Acquire the IPSNs from the management platform's database.
3. Store IPSNs in VNS database.
4. For each MAC address acquired from CAMs, get an IP address from the management platform.
5. If there is no MAC in the management platform's database, get an IP according to the MAC to IP address resolution procedure see 3.6.2.
6. Build an IPSN to VLAN map and a Port to VLAN map according to Fig. 4.
7. Display the map to the user for confirmation or modification.
8. Perform the VLAN assignment according to the Port to VLAN map generated in step 6.

3.6.4. Change Management in IP Network

A change in the IP network is defined as one of the following cases:

1. A new host appears
2. An existing host changes its IP address
3. A host moves to another port during the work (if a host is powered off and then moved, we consider this to be the case of new host)
4. A new IP Subnet is added

When a change occurs, the VLAN may be reassigned to the relevant port. A contradiction may occur during the change. For example, the VLAN of the station that caused the change, obtained from the IPSN2VN map, may contradict the previous VLAN assignment of the port due to other stations connected to the same port which already have a VLAN.

The system operates as follows: if there is no contradiction, assign the VLAN according to the IPSN2VN map. If there is, assign the global VLAN to the port and inform the user.

There are two sources of change detection: CAM change trap sent by management agent (see 2.2) and periodic frequent ARP requests sent by the station which connectivity problems. ARP requests are considered to be frequent if they are sent more than 5 times within 10 seconds. Such ARP requests are sent by a new station or the station whose IP address has been changed. A station that was moved to another port also transmits frequent ARPs but it may take up to 20 minutes until it starts to do this. Therefore, the detection basis for each case of change is:

1. New station- CAM change trap and frequent ARP requests
2. IP address change- frequent ARP requests
3. Station move- CAM change trap
4. New IP Subnet- Indication from the management platform

The CAM change trap gives an exact indication of port, on which the change occurred. ARP requests indicate MAC and IP addresses of the station that lost connection, but does not, of course, indicate its port.

While handling frequent ARP requests, the VNS looks in its database for the obtained MAC address. If the MAC is not found, or is found in database, but is missing in the CAM of the port that this station is supposed to be connected to, there is nothing to do and the VNS just continues to listen for changes and to perform the polling. When the problematic MAC is detected in the CAM, the change management is performed. This case of contradiction between the database information and the CAM content means that the CAM change trap was not received.

If a new IP Subnet is added to the router, the VNS detects it from the management platform. The new IPSN is added to the Net2VN table. If there are no other stations on the port of the router's interface with the new IPSN, the new raw is added to Net2VN along with the new VLAN number. If there are other IPSNs on this port, the new IPSN is added to the raw of the Net2VN table that contains these IPSNs.

The following change management process handles all the types of change.

1. Listen for CAM change traps.
2. Listen for frequent ARP requests.
3. When a CAM change trap is received:
   3.1. Acquire the CAM of the port specified in the trap.

3.2. Update CAM content in the VNS database.

3.3. Compare the new CAM with the one registered in the VNS database.

3.4. If there is no new MAC, then some station was deleted from the CAM. Go to 1.

3.5. Get IP address for the MAC according to the MAC to IP resolution procedure (see 3.6.2)

3.6. Go to 6.

4. When frequent ARP requests are detected:

4.1. Get MAC and IP addresses from the ARP packet.

4.2. Look in the VNS database for the MAC and the port and connect them.

4.3. If MAC is not found, Go to 1.

4.4. Acquire the CAM of the port and compare the new CAM with the CAM registered in the VNS database.

4.5. If the CAMs are identical (IP address change case), go to 6.

4.6. Update the CAM in database.

4.7. If there is no MAC in the new CAM, Go to 1.

4.8 Go to 6.

5. When the new IPSN is registered by the management platform:

5.1 If there are other IPSNs on the port of the relevant router interface, add the IPSN to the raw of the Net2VN table with these IPSNs.

5.2. Otherwise, add the new raw to Net2VN table.

5.3. Go to 6.

6. Assign the VLAN according to the following rule: if there is no contradiction, assign the VLAN according to the IPSN2VN map. If there is, assign the global VLAN to the port and inform the user.

7. Go to 1.

3.7. Novell Network

3.7.1. General Principles

Novell network configuration principles and the method of their implementation in a switch/routing environment are different from those in IP network. In a normal Novell environment different IPX Nets cannot be defined on the same Switch Fabric without vlans just as they can not be defined on the same Ethernet segment. If such a configuration is defined, the Novell servers periodically point out the IPXNs contradiction and do not recognize each other. This means that the user who initially connected to one server cannot log into another server even though they are connected physically.

The only way to use routing in a switched Novell Network is working with vlans.

The network manager may configure manually the IPXNs for each interface of all servers/routers. Then the VNS performs the VLAN configuration for all Novell servers, routers and stations.

As mentioned above, servers'/routers' interfaces with different IPXNs cannot work properly on the same physical segment because they mistakenly receive each other's messages. On the other hand, the server/router interface with the same IPX Net may get the same VLAN so that they can communicate directly. That leads us to the following two rules of VLAN assignment:

Rule 1: Server/router interfaces can not be in Global mode

Rule 2: For server/router interface: One and Only One IPX Net = VLAN

As in an IP Network, a workgroup consists of users who belong to the same IP Subnet. In a Novell Network a workgroup consists of the server and the users that logged into this server. Therefore, the general principle of VLAN assignment for Novell stations is:

Station VLAN = Server VLAN

Novell users can log into one server and then attach to up to 7 other servers. It is impossible to pre-define which servers the client will use most often. Therefore, for each port a dominant server is defined as the server with the largest number of clients from among the Novell stations connected to that port. Thus, we can state the following rule for station VLAN assignment.

Rule 3: Station VLAN = Dominant Server VLAN

3.7.2. VLAN Balance for Multiple-NIC Server

A Novell server may have more than one NIC. For proper NetWare functions, every NIC may be configured on a different IPXN. If the dominant server has more than one NIC, its client may get the proper VLAN assignment according to any NIC assignment. In order to balance the traffic between the NICs, the following simple balance principle is used: each NIC has an equal number of clients. The VLAN assignment rule is:

Rule 4: Station VLAN = VLAN of Dominant Server's NIC with Minimum Stations

For example, if the server has two NICs, the first client gets the VLAN of the first NIC, the second client gets the VLAN of the second NIC, the third - of the first NIC, the fourth - of the second NIC, etc.

3.7.3. VLAN Assignment Example

Fig. 6 illustrates VLAN assignment in the Novell network. Assume that the Novell network contains two servers, S1 and S2, and three clients: C1, C2 and C3. Server S1 has two NICs: the first configured on IPXN1 and the second on IPXN2. Thus, S1 is both a server and a router. Server S2 has one NIC which is configured on IPXN2. At the first stage The VNS assigns vlans to all server NICs according to the table:

IPXN	VLAN
1	1
2	2

Stations C1 and C2 are logged into S1, and C3 into S2. The VLAN assignment is performed in the following way. C3 gets VLAN2 according to the VLAN assignment of S2, its dominant server. C1 and C2 may be put on VLAN1 or VLAN2 because their default server S1 can be reached on both VLANs. According to rule 4, we must distribute the clients evenly. Therefore C1 is put on VLAN1 and C2 on VLAN2.

3.7.4. Problematic Connection Cases

Following are some cases of wrong or non-optimal connection of servers/stations to LANSwitch ports.

3.7.4.1. Servers on the Same Port

If more than one server interface, with different IPXNs, are connected to the same port, it is impossible to assign different VLANs to them because the LANSwitch port can get only one VLAN. Such a situation is problematic. Therefore, the following rule is checked by the VNS.

Rule 5: Server/router Interfaces with Different IPX Nets Can Not be on the Same Port

The VNS detects any violations of Rule 5 and announces them to the network

manager. The announcement makes the network manager aware of any connection problems. For example:

The servers DEVEX with IPX Net 2 and EMBEDDED with IPX Net 10 are connected to the same LANSwitch port: Hub LannetA, slot 2, port 1. Please, connect them to different ports.

3.7.4.2. Clients of different servers on the same port

If, according to the VLAN assignment systems described above, several stations get different VLANs and they are connected to the same port, a minimal hops procedure is implemented to define an optimal VLAN configuration. If there are routes from any station to its server, then any station can reach its server on any VLAN. In this case the rule of VLAN assignment is:

Rule 6: On one Port - Minimize the Sum of the Hops Needed for Each Station to Reach the Server

The minimal hops principle overwrites the balance principle, because balance cannot be implemented for stations on one port.

In Fig. 7 C1 logged into S1, C2 in S2. C1 and C2 are connected to the same port. Both VLAN1 and VLAN2 are good for proper connectivity. If VLAN1 is assigned to the port, the station C1 reaches S1 directly and C2 reaches S2 via S1. If VLAN2 is assigned, both C1 and C2 reach their servers directly. According to the minimal hops principle, VLAN2 is chosen.

The following chapter is intended to explain what happens when the clients of the servers with different IPXNs are connected to the same port and there is no route between these IPXNs.

3.7.4.3. No-route Case

When the station tries to enter the network, it broadcasts a "Get Nearest Server" SAP request and establishes an initial connection with the first server to reply. Then it can log into any other server which is known to this "nearest" server. If there is no route between servers with different IPXNs (and different VLANs, according to Rule 2), they do not know each other. The station can log only into the server with which it made initial contact and with the servers known to the initial server. The only way to ensure that the station will log into the necessary server is to define a preferred server in the initial configuration file of the station using the preferred server shell. When the preferred

server is defined, the station waits for the "Give Nearest Server" response from the preferred server.

In the no-route case, the station can reach the server only if it has the VLAN of the server or it is in Global mode. Thus, the right way to work in the no-route case is to define a preferred server for the station and to put the station on the server's VLAN. Preferred server definition can be done only by the network manager. VLAN assignment is done by the VNS.

If there is more than one station on the port that has to log into different servers which do not have routes to the other servers, the only way to provide the proper connection is to put the port on Global mode. Thus, the following rule is concluded:

Rule 7: In the "No-Route Case" Port with Different Servers' Stations may be in Global Mode

Figure 8 illustrates this case.

In this example there are no routes for C1 and C2 to reach their servers. They can reach them only directly: C1 on VLAN1 and C2 on VLAN2. If they are on the same port, the only way to connect them is Global VLAN assignment to the port.

In the "no-route" case, a new station that does not succeed to establish an initial connection is put on Global. After it has successfully logged in, it gets the VLAN of its server if there are no other stations using other servers on the same port . If there are, the station remains Global according to the Rule 7.

3.7.4.4. Station and Server on the Same Port

If a station and its server are connected to the same port, the station logs into the server successfully because it has the same VLAN as the server and the VNS has nothing to do here. If the station wants to log into a server connected to another port with a different VLAN and there is no route between these two servers, it never succeeds because the servers do not know about each other. the VNS can not detect this problem. We can just recommend to the network manager not to put on the same port a server and stations which need to work with other servers.

If there is a route between the servers, the station succeeds to log into the other server via the router and it is wrong to assign the VLAN of the second server to the station because this destroys the initial assignment of the first server which is on the same port as the station. The VNS might not change the VLAN of the port even though it would enable direct access of the station to the desired server. The following rule

summarizes this issue:

Rule 8: Server VLAN Assignment Cannot be Overwritten by Station Assignment

Fig. 9 illustrates the situation when the server and the station are connected to the same port. If the station C1 logs into server S1, it succeeds and there is nothing to do for the VNS. VLAN1 is already assigned to C1 because the server assignment has already been done. If C1 wants to log into S2 which is on VLAN2, it never succeeds because in this example there is no route from C1 to S2. C1 receives from S1 the response: "*Unknown server S2*". The VNS cannot detect such a situation.

3.7.5. VNS Functions in Novell Network

3.7.5.1. Servers Learning

In order to locate the Novell file servers, the VNS will periodically send "Get Nearest Server" SAP broadcasts. All Novell Servers that reply to this request will be registered by the VNS. The names, internal IPXN and external IPXN, of the servers will be obtained from the reply packet.

In order to learn the IPX routers, the VNS will periodically send "General Request" IPX RIP broadcasts. All IPX routers that reply to this request will be registered by the VNS. The IPXN of the router interfaces matched with the MAC addresses will be obtained from the reply packet.

3.7.5.2. Server Connections Learning

Server connection is the identification of the client logged into the server. (NetWare command USERLIST /A run on a client workstation provides a list of server connections.) The following parameters of server connections are used by the VNS for determining which clients are logged into the server.

Client Parameter	Usage
MAC Address	Get the server of the client with MAC obtained from CAM
IPXN	Determine the IPXN of the client

Server connections are identified only for the servers of type "file server". In order to identify client-server connections, the VNS will query the file servers via a "Get Internet Address" NCP request. MAC addresses and the IPXN of the clients will be obtained from the NCP replies.

3.7.5.3. Initialization

Initialization is the process of VLAN assignment to Novell servers, routers and stations, that have already logged into some server.

The following procedure is implemented on the initialization phase.

1. Identify all Novell servers/routers and routes by listening for SAP/RIP broadcasts.
2. For each server/router build an IPX Net - VLAN table according to Rule 2.
3. If Rule 1 or Rule 5 are not fulfilled, announce the user and stop.
4. For each server find all stations logged into it (see 3.7.5.2).
5. For each station:
   - 5.1. If there are clients of the servers with different IPXNs on the port:
     - 5.1.1. and it is the "no-route case", put the port on Global.
     - 5.1.2. Otherwise, find the optimal VLAN according to the minimum hops principle (Rule 6).
   - 5.2. If the server of the client has more than one NIC, assign a VLAN according to the balance (Rule 4).
   - 5.3. Otherwise (normal case), assign the VLAN of the default server.

3.7.5.4. Change management

Change in Novell network are defined as one of the following:

1. Adding a new server/router.
2. Moving an existing server/router
3. Changing the IPX Net of a server/router
4. Adding a new station
5. Moving an existing station

(Station/server moving is defined as moving while the station/server is in use. If the station is powered off and then moved and powered on, it is handled as a new station.)

For change detection the VNS uses different Novell broadcasts and CAM change trap. As in the IP case we say that protocol requests are frequent if they are sent more than 5 times in 10 seconds and have the same content.

For server change detection the VNS listens for periodic SAP broadcasts.

For router and route change detection the VNS listens for periodic RIP

broadcasts.

For detection of a station trying to establish an initial connection with the server, the VNS listens for frequent "Get Nearest Server" requests, transmitted by such stations approximately 40 times.

For detection of a station that lost its server connection, the VNS listens for frequent "RIP General Requests" transmitted by such stations approximately 40 times. To identify the server that the station is looking for it, internal IPX Net number is used. This number is extracted from the RIP General Request and the server is identified according to the information obtained from SAP broadcasts.

The CAM change trap is used as in the IP case to detect the port that the change occurred on, and to update the VNS database accordingly. No VLAN assignment is performed on the arrival of the trap because at the moment of arrival it is difficult to understand which change has taken place. If even after the change, the station is unable to connect, it is detected in one of three ways described above.

If the source of the change is a server, two cases of contradiction may occur. First, another server with a different IPX Net may be connected to the same port. Second, the stations using other servers may be connected to the same port and the new server may cause the no-route case.

The policy of server contradiction handling is: suggesting to the server to change the connection.

If the source of the change is a station, similar contradictions may occur. First, the necessary VLAN reassignment of the station may contradict the VLAN of the server residing on the same port. This case is considered to be the case of server contradiction and is treated according to the policy of server contradiction. Second, the VLAN reassignment of the station may contradict the VLAN of other stations connected to the same port.

The procedure of handling station contradictions is: if there is a route between the servers of the stations - do not change the VLAN. In the no-route case - put the station on Global.

In case of a new station that cannot get an initial connection no such contradictions can occur. If a server is connected to the station's port the station is connected to it. If other stations are connected to the port, the station is connected to one of their servers. Therefore, a new station that cannot get an initial connection with the server gets a global VLAN assignment.

The case of an IPXN change of server/router is discussed separately. Let us define two kinds of IPXN change: simple and complicated.

Simple IPX Net change is the change when some IPX Net number is changed to

another number for all servers'/routers' interfaces that had it. For example, IPXN3 was changed to IPXN5 for all interfaces previously configured on IPXN3.

Any other change is considered to be complicated.

The procedure of handling an IPXN change is: if the change is simple - update the Net2VN map, if it is complicated - inform the user, recommending to perform initialization again.

Notice that after the IPX Net change, the server may be rebooted. After rebooting the server, the stations connected to it may be rebooted also.

The following is the change management procedure, including all possible changes.

1. Listen for SAP and RIP broadcasts to detect server/router changes.
2. Listen for General RIP Requests to detect the station that lost its connection.
3. Listen for Get Nearest Server broadcasts to detect any station trying to establish an initial connection with a server.
4. Listen for CAM change traps
5. When an SAP/RIP broadcast is received:
  5.1 If no changes are detected, go to 1.
  5.2 If a new server is detected:
    5.2.1 If the new server has a new IPX Net, inform the user, proposing to perform initialization again.
    5.2.2 Otherwise (the existing IPXN):
      5.2.2.1. If there are no other stations, assign the VLAN according to the Net2VN table.
      5.2.2.2 If there is a route from the new server to the servers of other stations on the port, assign the VLAN according to Net2VN table.
      5.2.2.3. Otherwise (no-route), inform the user.
      5.2.2.4. Go to 1
  5.3 If an IPXN change is detected
    5.3.1 If it is simple change, just update the Net2VN map
    5.3.2 Otherwise (complicated change), send an announcement to the user
    5.3.3 Go to 1.
6. If Get Nearest Server requests are detected
  6.1. Put the station on Global and send an announcement to the user.
  6.2. Go to 1
7. If General RIP Requests are detected (station moved to another port)
  7.1 Determine which server the station is looking for.

7.2 If there is a server contradiction, announce it to the user.
7.3 If there is a station contradiction, put the station on Global
7.4 Otherwise (no contradictions), assign the VLAN of the server
7.5 Go to 1

8. CAM change trap detected
8.1. Perform steps 3.1-3.4 of change management for IP
8.2 Go to 1

3.8. Mixed IP-Novell Network

3.8.1. General

A mixed IP-Novell environment has become very popular today. First, people add IP stations to Novell networks and vice versa -i.e. Novell servers and stations to IP networks. Second, TCP/IP packages are often installed on Novell servers and stations. Such a station becomes both Novell and IP node. Third, there are software packages that add to UNIX stations with native TCP/IP environment the possibility to serve as a Novell server or client, e.g. SolarNet of SunSoft.

Due to these facts, we may take care of the proper VNS functions in a mixed IP-Novell network. Taking into consideration the rules and the procedures defined above for pure IP and pure Novell environments, we can construct mixed procedures and define the VNS behavior in a mixed network.

3.8.2. Mixed Net to VLAN Mapping Procedure

A mixed IPSN-IPXN to VLAN mapping procedure is much more complicated than an IPSN to VLAN mapping procedure. The mapping procedure for a pure IP network may always succeed. A mixed procedure could fail for any of the reasons described below. If it fails, the VNS informs the user about the reason for failure and stop initialization. It is up to the network manager to change the connection and run initialization again.

The main reason that the procedure could fail is violation of Rule 2. It may happen that according to the IPSN to VLAN mapping procedure principle, different IPXNs may get the same VLAN. For example, port 1 may connect IPSN50 and the server with IPXN1, and port 2 may connect IPSN50 and the server with IPXN2. In order to provide connections for IP stations, ports 1 and 2 may get the same VLAN. On the other hand, they may get different VLANs according to Rule 2. We call such a contradiction IPSN-IPXN contradiction. There is no way to solve this contradiction and the procedure announces it to the network manager and stops.

The mixed procedure is based on division of the stations into three types: IP station, Novell server and Novell client. Each type of station gets special processing according to the following priorities.

The Novell servers have priority and are processed first. A Server2IPXN index mapping servers to their IPXNs is built and an IPXN to VLAN mapping is performed according to IPXN configuration of the servers and their connections. The result is inserted into the Net2VN and Port2VN tables.

The IP stations have second priority and are processed in the second step. The processing of the IP stations is performed by three passes. In the first pass, the ports that were assigned VLANs during server processing are handled. The IPSNs connected to these ports are added to the Net2VN table according to the IPXN to VLAN assignment. The IPSN-IPXN contradictions are checked in this pass. In the second pass the IP to VLAN mapping procedure is activated based on the previously assigned ports. In the third pass, the IP to VLAN mapping procedure is activated for still unassigned ports. Server ports are not touched here because they have been already covered in the first and second passes.

<u>1. Step 1 (Novell servers)</u>

1.1 Build the Server2IPXN index

1.2 Build the IPXN to VLAN mapping and insert it into the Net2VN and Port2VN tables.

<u>2. Step 2 (IP stations)</u>

2.1 Pass One (IP stations on server ports)

2.1.1 Build the Net2Port index for the IPSNs.

2.1.2 Build the Port2Net index, notifying servers and clients.

2.1.3 For each assigned port:

2.1.3.1 For each IPSN in Port2Net[port]:

2.1.3.1.1 If already assigned, the IPSN may get another VLAN, announce the IPSN-IPXN contradiction and stop.

2.1.3.1.2 Add the IPSN to the appropriate entry of the Net2VN table

2.2 Pass Two (IPSNs of the server ports on the other ports)

2.2.1 Activate the IP to VLAN mapping procedure for each already assigned port.

2.2.1.1 If two IPSNs that have already been assigned different VLANs are detected on one port, put the port on Global (it can not be the server port)

2.3 Pass Three (Remained IPSNs)

2.3.1 Activate the IP to VLAN mapping procedure for all unassigned ports

<u>3. Step 3 (Novell clients)</u>

3.1 Pass remained ports (client ports)

3.1.1 If there are clients of different servers on the port

3.1.1.1 If in the no-route case, put the port on Global

3.1.1.2 Otherwise, find the optimal VLAN by the minimal hops principle

3.1.2 If the server of the client has more than one IPXN, assign the VLAN according to the balance principle.

3.1.3 Otherwise (normal case), assign the VLAN of the default server

3.8.3. Initialization in a mixed IP-Novell network

The following procedure is implemented for the initialization phase in a mixed IP-Novell network.

1. Identify and poll the management agents for the LANSwitch parameters thereby updating the VNS database
2. Acquire the IPSNs from the management platform's database
3. Store IPSNs in VNS database.
4. Identify the Novell servers/routers (see 3.7.1).
5. If Rule 1 or Rule 5 are not fulfilled, send an announcement to the user and stop.
6. For each Novell server Identify the stations that are logged into it (see 3.7.5.2).
7. For each MAC address acquired from the CAMs
   7.1 Look for the corresponding IP address in the management platform
   7.2 If not found, try to get the IP according to the MAC to IP address resolution procedure.
   7.3 If not found, assume that it is not the IP node
8. Activate the mixed Net to VLAN mapping procedure to build the Net2VN and Port2VN tables
9. Display the map to the user for confirmation or c change
10. If the user changed the map, edit the Port2VN table accordingly
11. Perform the VLAN assignment according to the Port2VN table

3.8.4. Change Management for mixed IP-Novell network

Change management in a mixed IP-Novell network is simply a matter of uniting the change management procedures for the pure IP and pure Novell networks. Due to the "callback" nature of the change management, it is easy to unite these two procedures. The formal description of the procedure begins by listening for various kinds of changes. When a change is detected, it is processed as in the pure environments.

1. Listen for SAP and RIP broadcasts to detect server/router changes.

2. Listen for General RIP Requests to detect the station that lost its connection.

3. Listen for Get Nearest Server broadcasts to detect the stations that try to establish an initial connection with a server.

4. Listen for frequent ARP requests.

5. Listen for CAM change traps.

Definitions of some of the terms used in the above description are now provided:

Reserved ports -- User-designated ports within a network to which the system shown and described herein does not assign VLANs.

Backbone ports list -- list of all backbone ports within a network i.e. a list of all ports within a network which connect one switching hub to another, as opposed to ports which connect end-stations to switching hubs.

Net -- an IP subnetwork (IPSN) or an internal packet exchange network (IPXN).

Net2VN map or Net2VN table -- a table mapping a VLAN to each subnet in a network.

Port2VN table or Port2VN map -- a table mapping a VLAN to each port in a network.

IPSN2VN table or IPSN2VN map -- a table mapping a VLAN to each IPSN in a network.

IPXN2VN table or IPXN2VN map -- a table mapping a VLAN to each IPXN in a network.

Global VLAN (or GN or global VN) -- A VLAN that communicates directly with all VLANs defined for an individual network.

Fig. 13 is a screen generated by a VLAN assigning system for a network including 4 IP subnets and 3 IPX networks. The display of Fig. 13 includes, for each IP subnet or IPX network, its network address, a previous VLAN to which the subnet or network was assigned according to a previous VLAN assignment scheme, and a proposed VLAN to which the subnet or network is assigned according to the VLAN assignment scheme generated by the software embodiment.

Reference is now made to Fig. 14 which is a screen generated by a VLAN assigning system which prompts a user to define reserved ports to which no VLAN is to be assigned. Once the user has assigned one or more reserved ports, the system generates a VLAN assignment scheme according to which only components of the network other than the reserved ports are assigned to VLANs. The system typically operates as it would if reserved ports had not been assigned, i.e. the system operates as it normally would for a network in which the reserved ports are absent.

According to a preferred embodiment of the present invention, apparatus for managing a switched routed network is provided which includes:

a. a network configuration learning unit operative to learn a configuration of a switched routed network including an existing division into VLANs. The network configuration learning unit comprises a diagnostic unit for analyzing and diagnosing the existing division of the network into VLANs.

b. a VLAN assignment unit for generating a new division of the network into virtual LANs (VLANs) based on the learned configuration of the network.

Fig. 15 is a preferred method of operation for VLAN assignment apparatus constructed according to the above-referenced embodiment. The method of Fig. 15 identifies the subnets into which the network is divided by analyzing each network address detected in the network. For each such subnet, the method determines the VLAN or VLANs associated therewith in the existing division of the network. The method is also operative to find, for each VLAN identified, all ports associated with that VLAN. Unless only one VLAN is found, the method is operative to identify contradictions in the information it finds. For example, if a single subnet is found to be associated with more than one non-global VLAN, this is a contradiction. Another example of a contradiction is a Novell server which belong to different IPX networks and are found to be connected to ports assigned to a single VLAN. Yet another example of a contradiction is an IPX router belonging to different IPX networks which are found to be connected to ports assigned to a single VLAN.

Referring again to Fig. 3, the method shown and described herein is preferably operative to perform a change management function by detecting at least one event at an individual network element including detecting the identity of the individual end-station. Events comprise any of the following:

a. A logical change such as a change in the IP address of an end-station.

b. A physical change. Examples of physical changes include adding a new end-station and moving an end-station from port to port.

c. A communication failure. Examples of communication failures include a failed attempt of a NetWare client end-station to initially connect to a server end-station, and disconnection of a NetWare client end-station from a server end-station.

Each event is preferably categorized as either problematic or non-problematic. If the event is problematic, a suitable warning is generated such as the warning on the screen display of Fig. 16. If the event is non-problematic, such as an end-station which has moved from a first port within a certain VLAN to another port which is within the same VLAN, a suitable message is also preferably displayed.

Preferably, the system is operative to detect a mismatch between the network

address of an end-station and a VLAN to which the port to which the end-station is connected belongs, to determine a new VLAN which matches the network addresses of all end-stations connected to the port, and to assign the new VLAN to the port.

Optionally, the system is operative to store a record of problematic and non-problematic events occurring at network elements. A record of a problematic event typically comprises, a description of a contradictory VLAN assignment associated with the problematic event and one of the following:

a. A recommendation describing how a human operator may resolve the contradictory VLAN assignment; and

b. A description of a system action which resolves the contradictory VLAN assignment.

It is appreciated that the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

CLAIMS

1. Apparatus for managing a switched routed network comprising:

a network configuration learning unit operative to learn a configuration of the switched routed network;

a VLAN assignment unit for generating a division of the network into virtual LANs (VLANs) based on the learned configuration of the network; and

a change manager operative to detect a change in the configuration of the network and to modify the division of the network into VLANs.

2. Apparatus according to claim 1 wherein the configuration of the network includes physical configuration aspects and logical configuration aspects.

3. Apparatus for learning the configuration of a switched routed network, the network comprising:

a switching skeleton including at least one switching hubs interconnected by a switch backbone, each switching hub including at least one port; and

a plurality of end -stations each having a unique physical address and each communicating with an individual one of the switching hubs via one of the switching hub's ports, thereby defining a plurality of end-station to port connections, the plurality of end-stations including at least one router,

the apparatus comprising:

a end-station to port connection learning unit operative to learn associations between ports and physical addresses of the end-stations communicating therewith;

a physical address - logical address association learning unit operative to learn associations between logical addresses and physical addresses; and

an end-station to logical address association learning unit operative to derive associations between ports and logical addresses from said learned associations between ports and physical addresses of the end stations and said learned associations between logical addresses and physical addresses.

4. Apparatus according to claim 3 wherein said physical address-logical address association learning unit is operative to:

scan physical addresses of at least some of said plurality of end stations; and

actively find an associated logical address upon encountering each physical address.

5. Apparatus according to claim 4 wherein each said logical address comprises an IP network layer address and wherein the network comprises an IP network which is partitioned into a multiplicity of IP subnets and wherein each IP network layer address belongs to an individual one of said multiplicity of subnets and wherein said apparatus for learning also comprises apparatus for determining all IP subnets into which the IP network is partitioned.

6. Apparatus according to claim 4 wherein each said logical address comprises an IPX protocol network layer address and wherein the network is partitioned into a multiplicity of IPX networks and wherein each IPX protocol network layer address belongs to an individual one of said multiplicity of IPX networks and wherein said apparatus for learning also comprises apparatus for determining all IPX networks into which the IPX network is partitioned.

7. Apparatus according to claim 5 wherein said physical address-logical address association learning unit is operative to send a multiplicity of ICMP echo request packets to each of at least some of said plurality of end stations, each echo request packet including a physical destination address and an IP network layer destination address which includes an IP broadcast address of an individual one of said multiplicity of subnets;

and wherein the echo request packet sent to an individual end station has a physical destination address which is the physical address of the individual end station.

8. Apparatus according to claim 7 wherein said physical address -logical address association learning unit comprises an ICMP echo reply packet analyzer operative to derive a physical address - IP address association from each arriving ICMP echo reply packet.

9. Apparatus according to claim 6 wherein said physical address-logical address

association learning unit is operative to send an IPX diagnostic packet to each of at least some of said plurality of end stations, an IPX diagnostic packet including a physical destination address and an IPX network layer destination address which includes an IPX broadcast address;

and wherein the IPX diagnostic packet sent to an individual end station comprises an IPX diagnostic packet whose physical destination address is the physical address of the individual end station.

10. Apparatus according to claim 9 wherein said physical address -logical address association learning unit comprises an IPX diagnostic packet analyzer operative to derive a physical address - IPX address association from each arriving IPX diagnostic reply packet.

11. Apparatus according to claim 3 wherein said physical address-logical address association learning unit includes an IP network layer address identifier operative, for each physical address, to passively identify a logical address comprising an IP network layer address,

and wherein said IP network layer address identifier is operative to listen for ARP packets and to analyze the ARP packets and derive therefrom IP network layer addresses.

12. Apparatus according to claim 3 wherein said network comprises a NetWare network,

and wherein said plurality of end-stations comprises at least one NetWare file servers and at least one NetWare clients,

and wherein each of the NetWare clients is served by one of the at least one NetWare file servers,

and wherein said apparatus for learning also comprises a server-client learner operative to identify servers and clients from among said plurality of end-stations and to learn relationships between said servers and said clients.

13. A method for generating a division of a switched routed network into virtual LANs (VLANs) based on a learned configuration of the network, the network comprising:

a switching skeleton including at least one switching hubs interconnected by a switch backbone, each switching hub including at least one port; and

a plurality of end -stations each having a unique physical address and each communicating with an individual one of the switching hubs via one of the switching hub's ports, thereby defining a plurality of end-station to port connections, the plurality of end-stations including at least one router,

the method comprising:

dividing the plurality of end-stations into nodes, wherein each node comprises a set of at least one end-station;

connecting each first and second node from among said nodes with an arc if at least one of the end-stations in the first node set is associated with the same port as at least one of the end-stations in the second node set, thereby to generate at least one disjoint graphs;

allocating a VLAN to each of the at least one disjoint graphs characterized in that packets sent by an individual end-station connected to a port belonging to an individual VLAN, including broadcast packets, are transmitted only to end-stations connected to one of the ports within the same VLAN.

14. A method according to claim 13 wherein the network comprises an IP network which is partitioned into a multiplicity of IP subnets and said sets respectively correspond to said IP subnets.

15. A method according to claim 13 wherein the network is partitioned into a multiplicity of IPX networks and said sets respectively correspond to said IPX networks.

16. A method according to claim 13 wherein the network comprises a NetWare network and wherein said plurality of end-stations comprises at least one NetWare file servers and at least one NetWare clients and wherein each of the NetWare clients is served by one of the at least one NetWare file servers, and wherein each of said sets comprises an individual NetWare file server and the NetWare clients served thereby.

17. A method according to claim 16 and wherein the VLANs are allocated so as to increase the number of clients which communicate directly with their servers rather than via a router.

18. A method according to claim 13 and also comprising the step of allocating global VLANs to at least one of the ports so as to reduce the number of end-station pairs which hear broadcast packets arriving to one another.

19. A method according to claim 18 and also comprising the step of allocating global VLANs to at least one of the ports so as to minimize the number of end-station pairs which hear broadcast packets arriving to one another.

20. A method for detecting a change in the configuration of a switched routed network, the network including a plurality of network elements, and for modifying a division of the network into VLANS, the method comprising:

detecting at least one event at an individual network element including detecting the identity of the individual end-station, the event comprising at least one of the following:

at least one logical change;

at least one physical change; and

at least one communication failure; and

categorizing at least one event as a problematic event or a non-problematic event and, if the event is categorized as problematic, alleviating the failure situation.

21. A method according to claim 20 wherein said at least one physical change comprises at least one of the following:

at least one new end-station added at at least one individual port within the network; and

at least one end-station which has moved from a first port within the network to a second port within the network.

22. A method according to claim 20 wherein said at least one logical change comprises an IP address of at least one end-station which has changed.

23. A method according to claim 20 wherein said at least one communication failure comprises at least one of:

a failed attempt of a NetWare client end-station to initially connect to a server

end-station; and

a NetWare client end-station which has been disconnected from a server end-station.

24. A method according to claim 20 wherein said analyzing and alleviating step comprises:

detecting a mismatch between the network address of an end-station and a VLAN to which the port to which the end-station is connected belongs; and

determining a new VLAN which matches the network addresses of all end-stations connected to said port; and

assigning the new VLAN to the port.

25. Apparatus for generating a VLAN assignment scheme according to which individual components of a network are assigned to VLANs, the apparatus comprising:

a reserved port designator operative to accept a user's designation of ports within the network to which no VLAN is to be assigned; and

a VLAN assignment scheme generator operative to generate a VLAN assignment scheme according to which only components of the network other than said reserved ports are assigned to VLANs.

26. Apparatus for managing a switched routed network comprising:

a network configuration learning unit operative to learn a configuration of a switched routed network including an existing division into VLANs; and

a VLAN assignment unit for generating a new division of the network into virtual LANs (VLANs) based on the learned configuration of the network,

wherein the network configuration learning unit comprises a diagnostic unit for analyzing and diagnosing the existing division of the network into VLANs.

27. Apparatus according to claim 26 wherein said diagnostic unit is operative to identify end-stations which belong to the same IP subnet and which are connected to ports assigned to different VLANs.

28. Apparatus according to claim 26 wherein said diagnostic unit is operative to identify Novell servers belonging to different IPX networks which are connected to ports assigned to a single VLAN.

29. Apparatus according to claim 26 wherein said diagnostic unit is operative to identify IPX routers belonging to different IPX networks which are connected to ports assigned to a single VLAN.

30. A method according to any of claims 20 - 24 and also comprising storing a record of problematic and non-problematic events occurring at network elements.

31. A method according to claim 30 wherein said record of problematic events comprises, for each problematic event, a description of a contradictory VLAN assignment associated with the problematic event.

32. A method according to claim 31 wherein said record of problematic events comprises, for at least one problematic event, a recommendation describing how a human operator may resolve the contradictory VLAN assignment.

33. A method according to claim 31 wherein said record of problematic events comprises, for at least one problematic event, a description of a system action which resolves the contradictory VLAN assignment.

34. A method according to any of claims 20 - 24 wherein said step of alleviating comprises alerting a human operator that a problematic event has occurred.

35. A method according to claim 30 wherein said step of alleviating comprises alerting a human operator that a problematic event has occurred.

FIG. 1

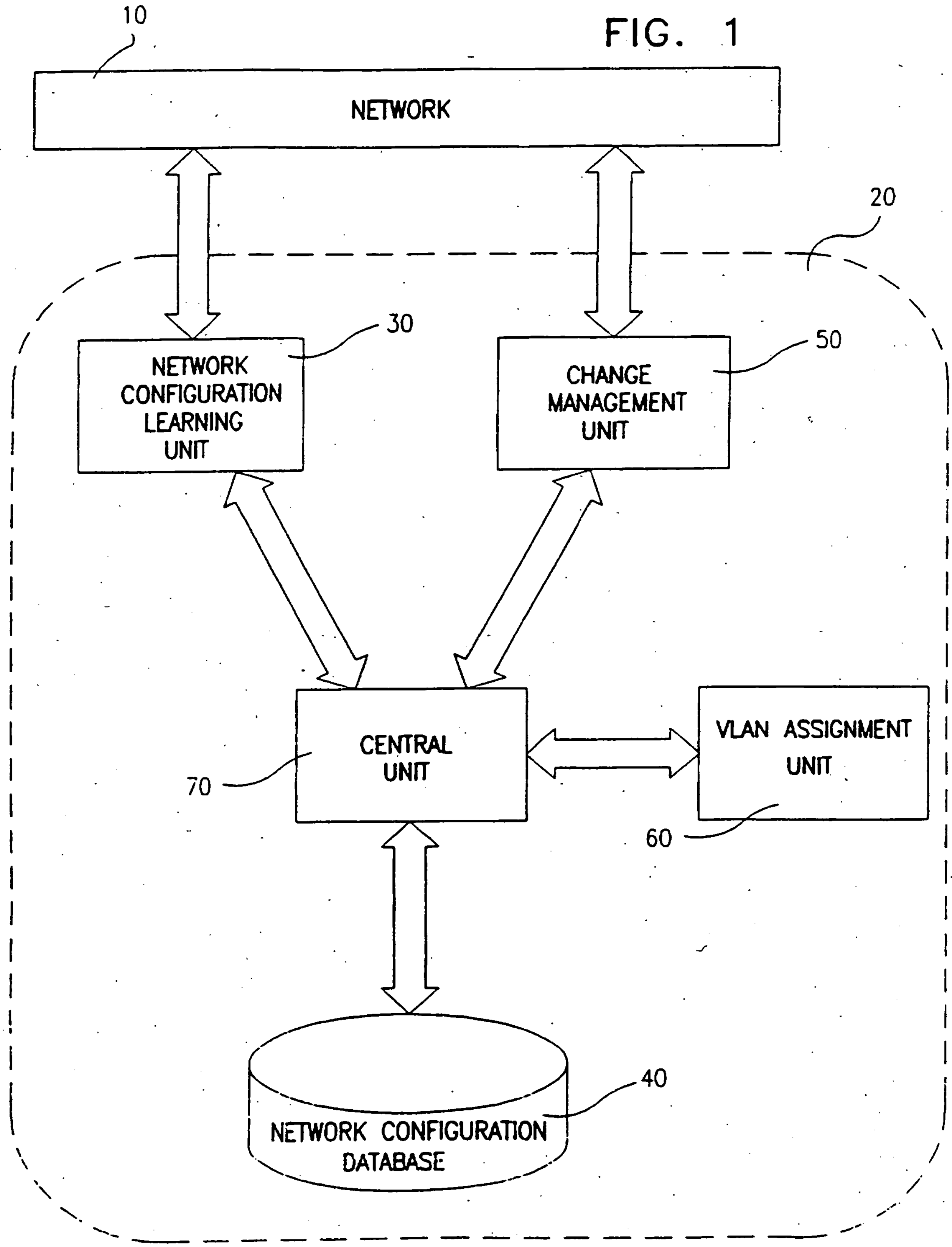

10
NETWORK
20
NETWORK CONFIGURATION LEARNING UNIT
30
CHANGE MANAGEMENT UNIT
50
CENTRAL UNIT
70
VLAN ASSIGNMENT UNIT
60
NETWORK CONFIGURATION DATABASE
40

FIG. 2A

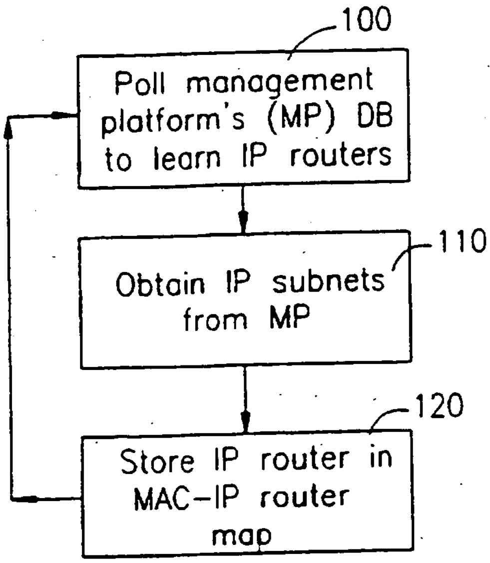


FIG. 2B

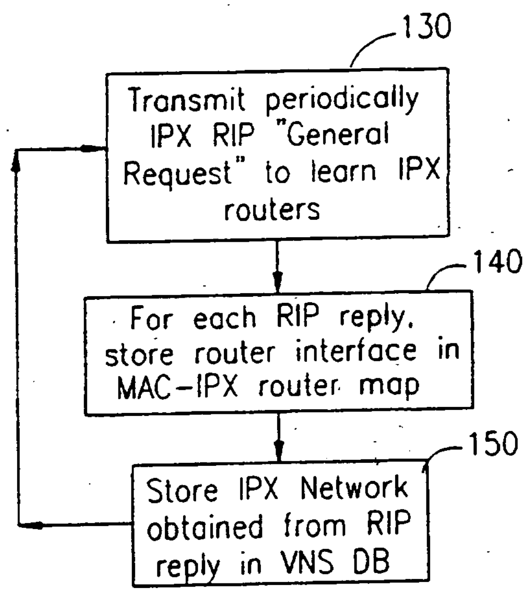


FIG. 2C

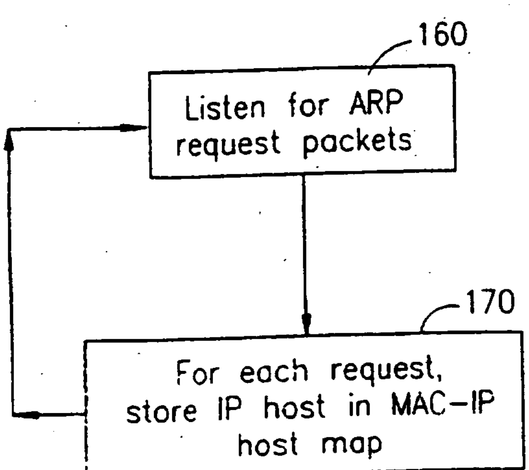
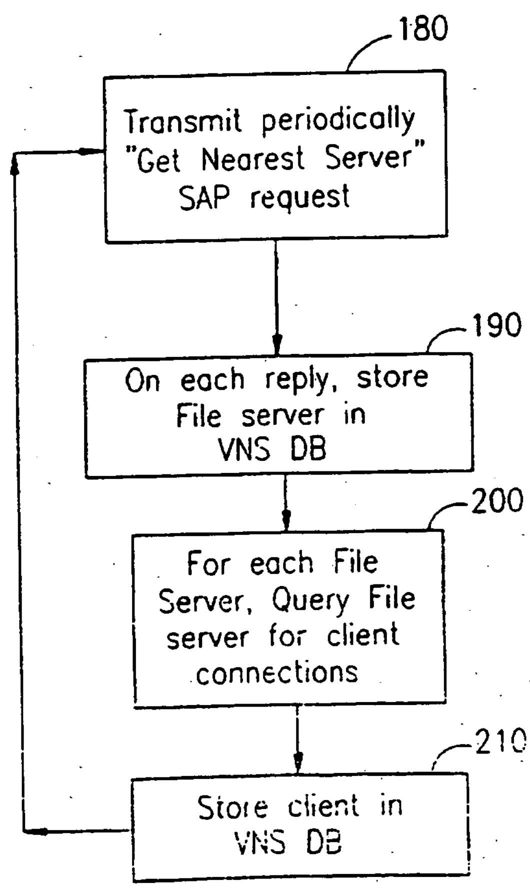
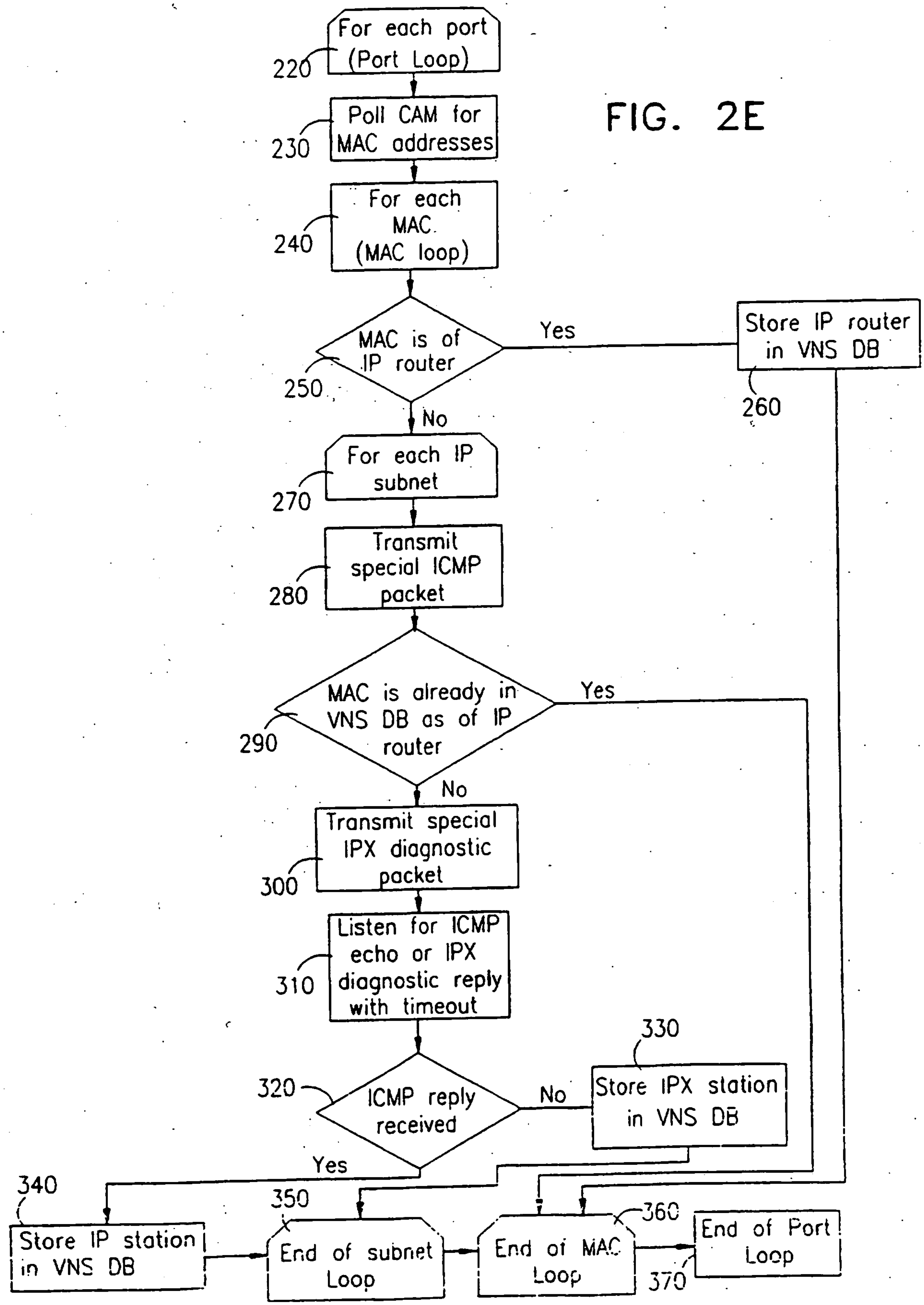


FIG. 2D





For each port (Port Loop)
220
Poll CAM for MAC addresses
230
For each MAC (MAC loop)
240
MAC is of IP router
250
Yes
Store IP router in VNS DB
260
No
For each IP subnet
270
Transmit special ICMP packet
280
MAC is already in VNS DB as of IP router
290
Yes
No
Transmit special IPX diagnostic packet
300
Listen for ICMP echo or IPX diagnostic reply with timeout
310
330
320
ICMP reply received
No
Store IPX station in VNS DB
Yes
340
Store IP station in VNS DB
350
End of subnet Loop
End of MAC Loop
360
End of Port Loop
370

FIG. 2E

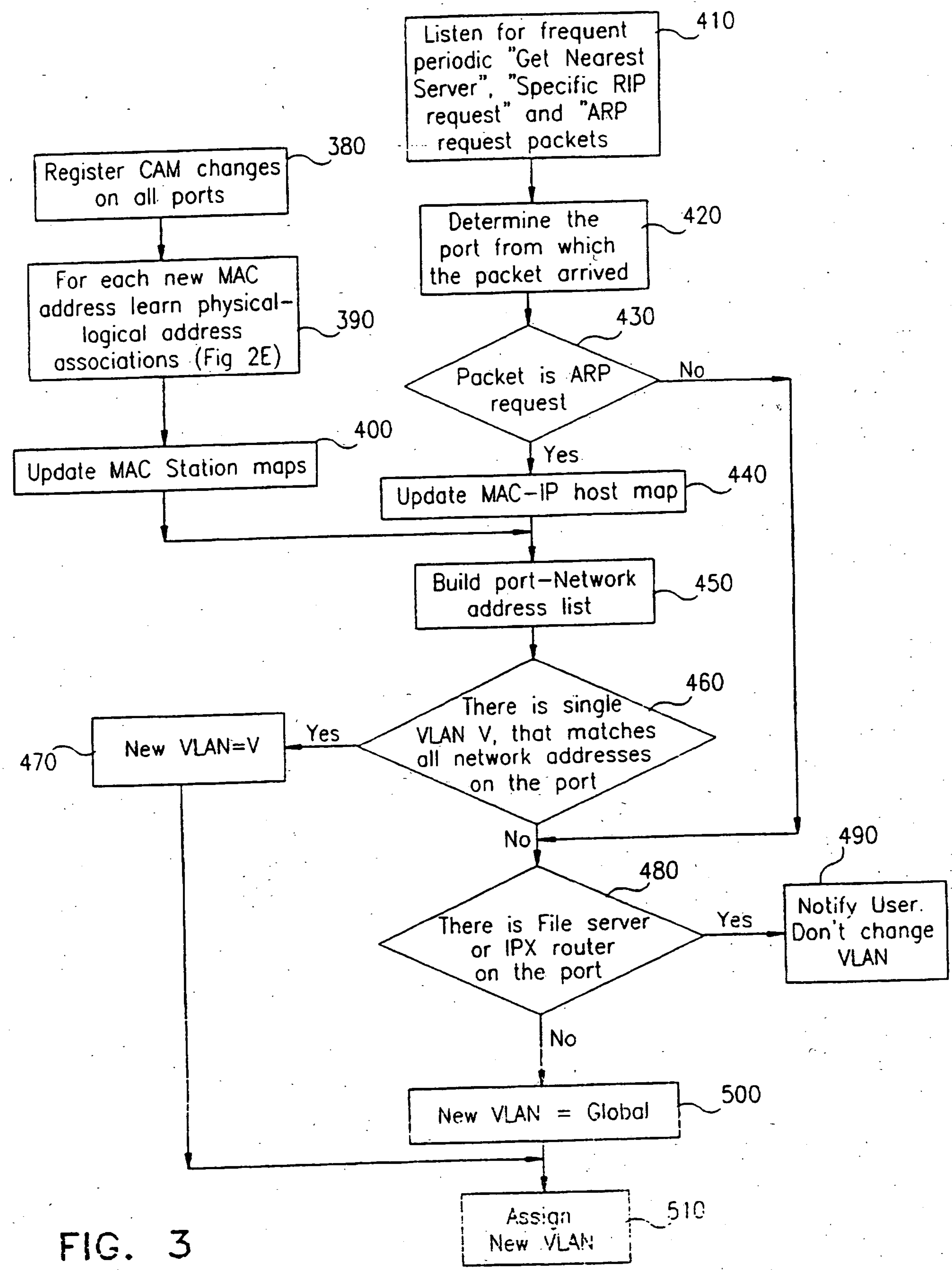

Listen for frequent periodic "Get Nearest Server", "Specific RIP request" and "ARP request packets
410
Register CAM changes on all ports
380
Determine the port from which the packet arrived
420
For each new MAC address learn physical-logical address associations (Fig 2E)
390
430
Packet is ARP request
No
Yes
Update MAC Station maps
400
Update MAC-IP host map
440
Build port-Network address list
450
460
There is single VLAN V, that matches all network addresses on the port
Yes
New VLAN=V
470
No
490
480
There is File server or IPX router on the port
Yes
Notify User. Don't change VLAN
No
New VLAN = Global
500
Assign New VLAN
510

FIG. 3

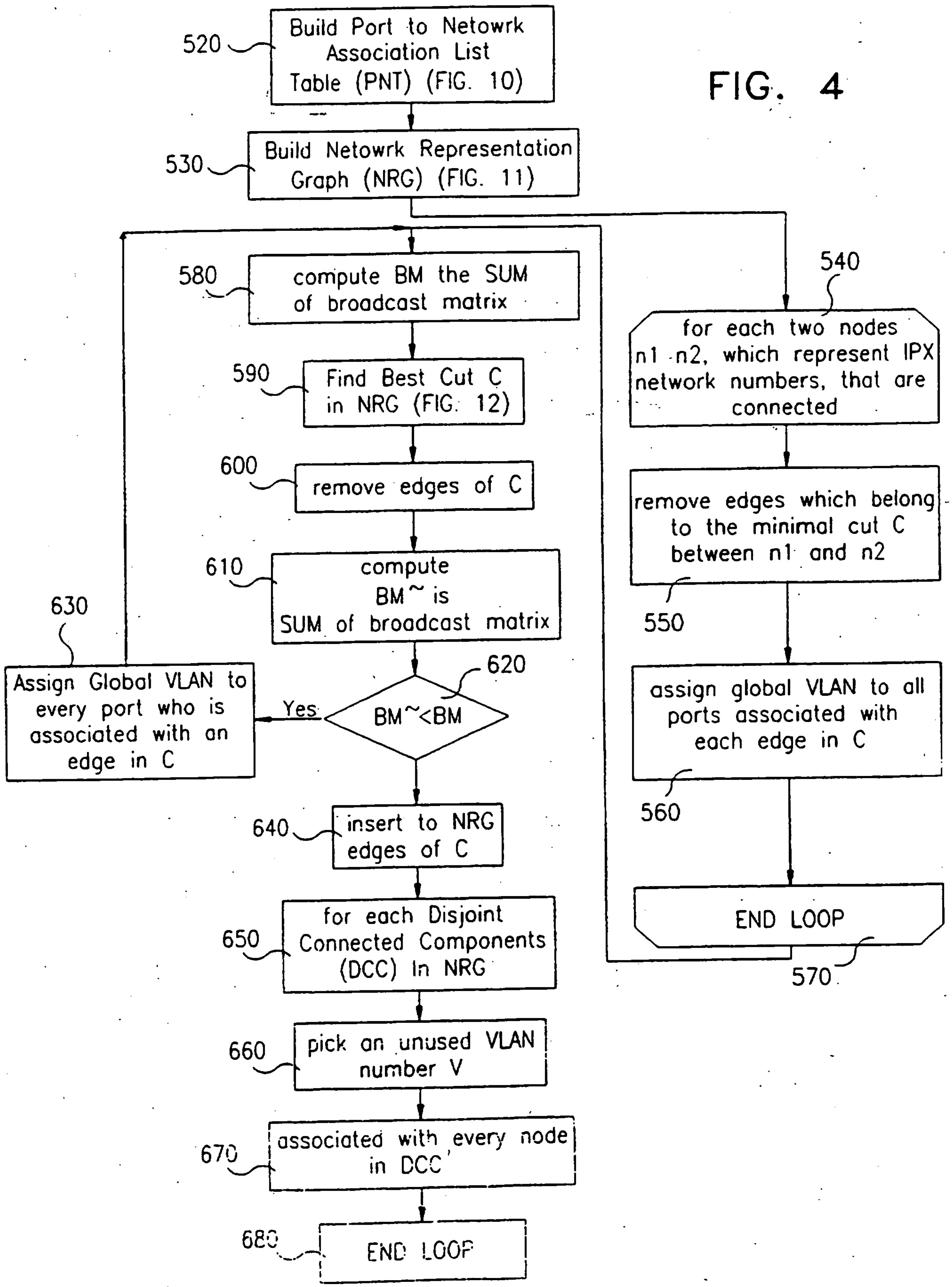
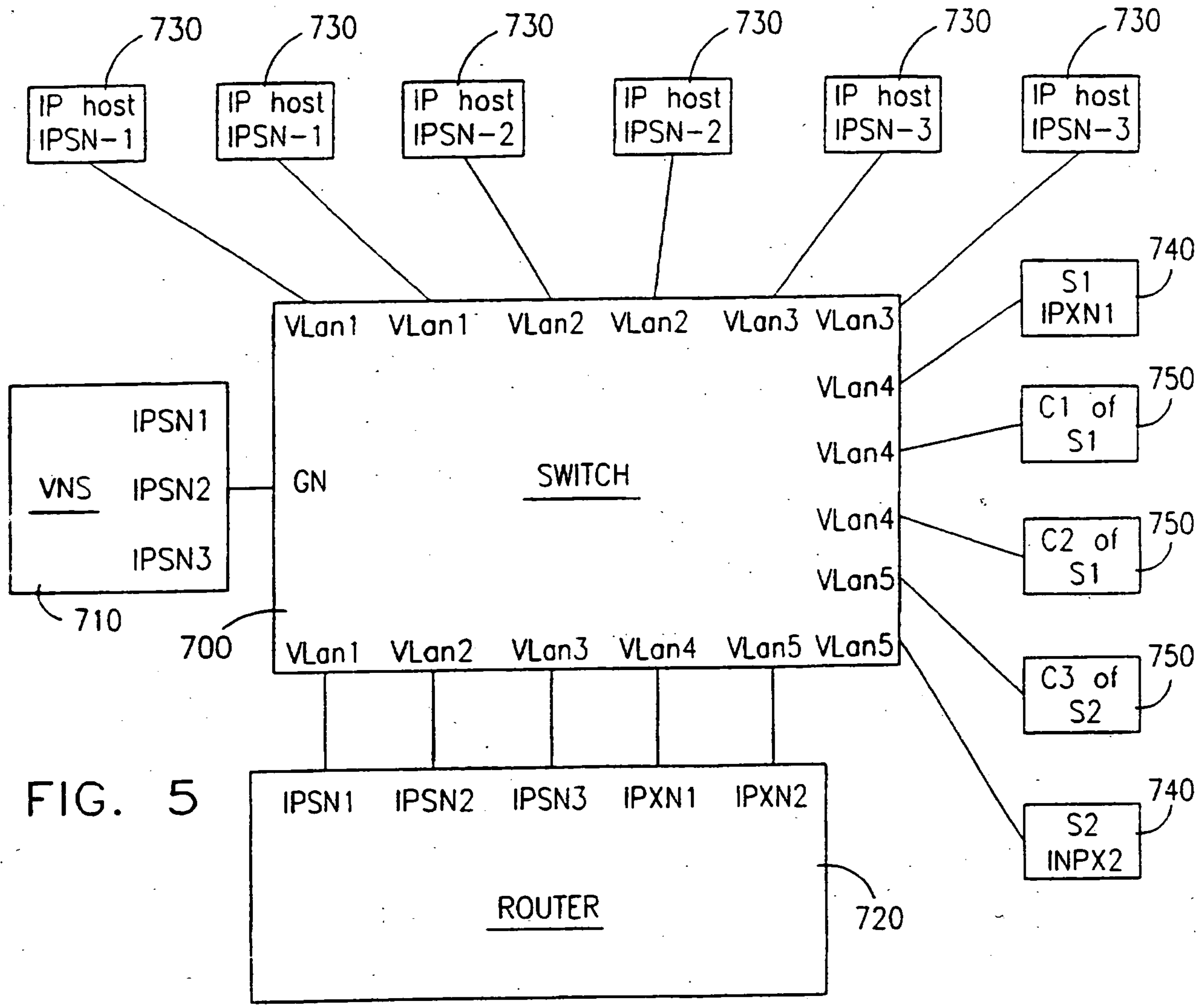
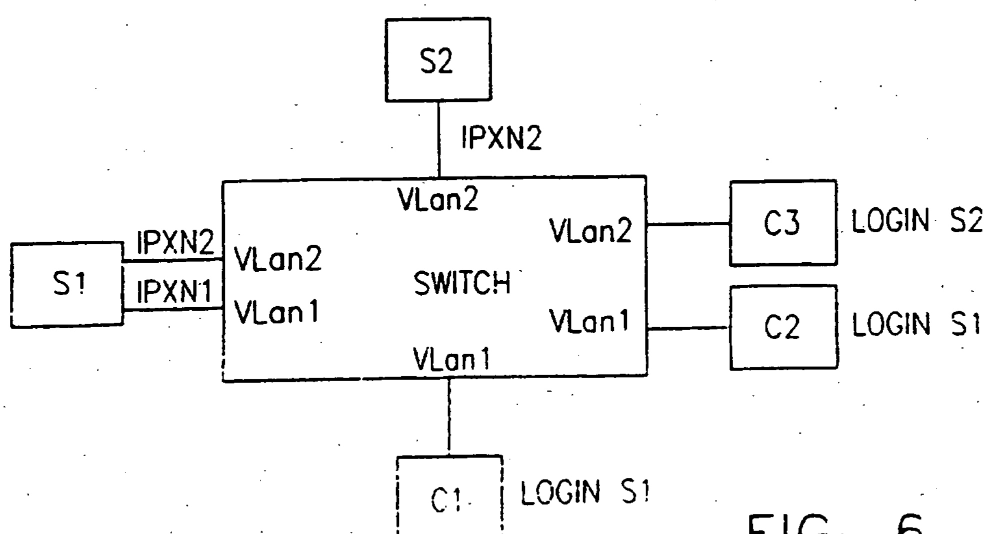

520
Build Port to Netowrk Association List Table (PNT) (FIG. 10)
530
Build Netowrk Representation Graph (NRG) (FIG. 11)
580
compute BM the SUM of broadcast matrix
590
Find Best Cut C in NRG (FIG. 12)
600
remove edges of C
610
compute BM~ is SUM of broadcast matrix
620
BM~<BM
Yes
630
Assign Global VLAN to every port who is associated with an edge in C
640
insert to NRG edges of C
650
for each Disjoint Connected Components (DCC) In NRG
660
pick an unused VLAN number V
670
associated with every node in DCC
680
END LOOP
540
for each two nodes n1 n2, which represent IPX network numbers, that are connected
remove edges which belong to the minimal cut C between n1 and n2
550
assign global VLAN to all ports associated with each edge in C
560
END LOOP
570

FIG. 4



730
IP host IPSN-1
IP host IPSN-1
IP host IPSN-2
IP host IPSN-2
IP host IPSN-3
IP host IPSN-3
VLan1 VLan1 VLan2 VLan2 VLan3 VLan3
VLan4
VLan4
VLan4
VLan5
VLan1 VLan2 VLan3 VLan4 VLan5 VLan5
740
S1 IPXN1
750
C1 of S1
C2 of S1
C3 of S2
S2 INPX2
VNS
IPSN1
IPSN2
IPSN3
GN
SWITCH
710
700
IPSN1 IPSN2 IPSN3 IPXN1 IPXN2
ROUTER
720

FIG. 5



S2
IPXN2
VLan2
VLan2
C3
LOGIN S2
S1
IPXN2
IPXN1
VLan2
VLan1
SWITCH
VLan1
C2
LOGIN S1
VLan1
C1
LOGIN S1

FIG. 6

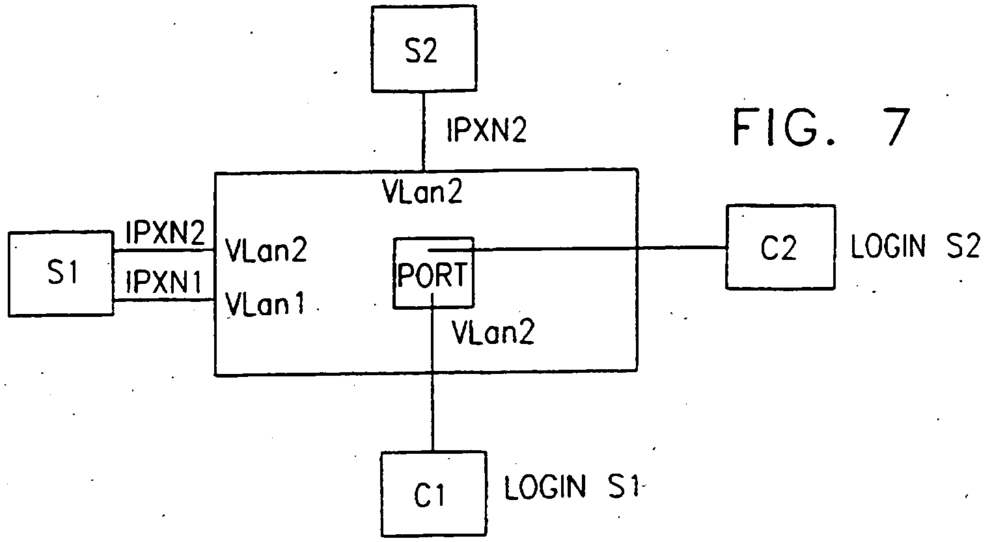


FIG. 7

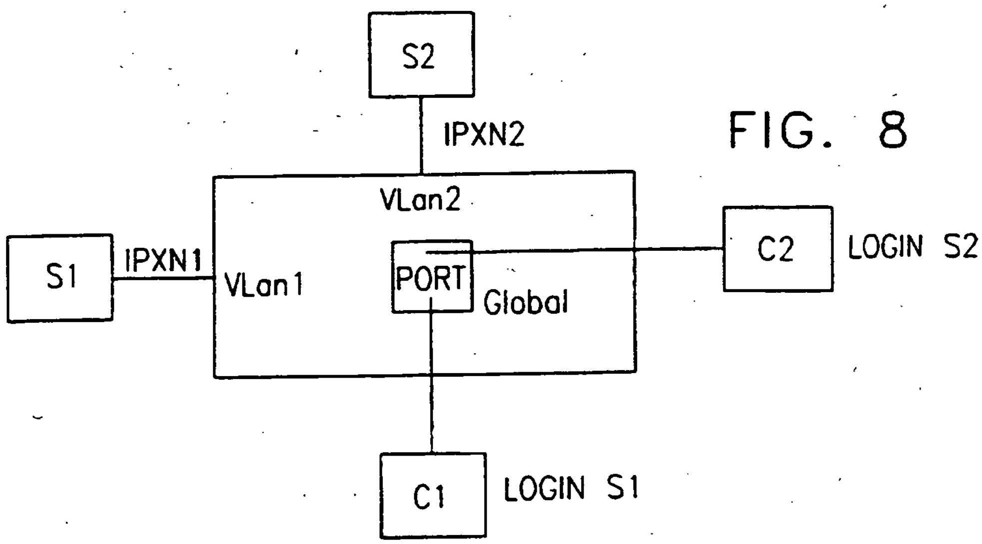


FIG. 8

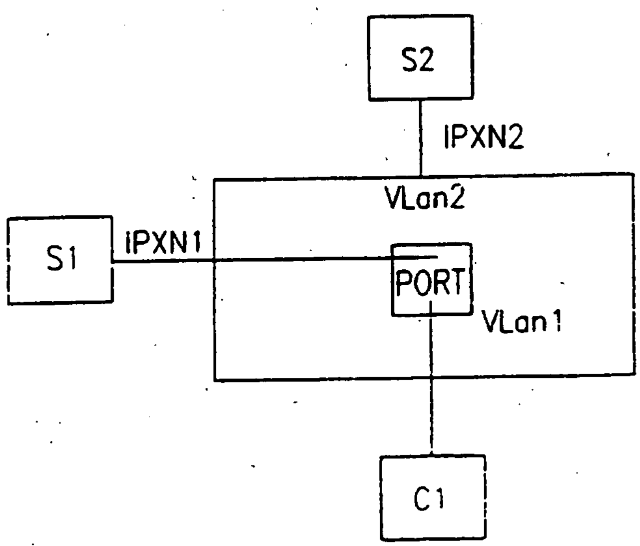


FIG. 9

FIG. 10

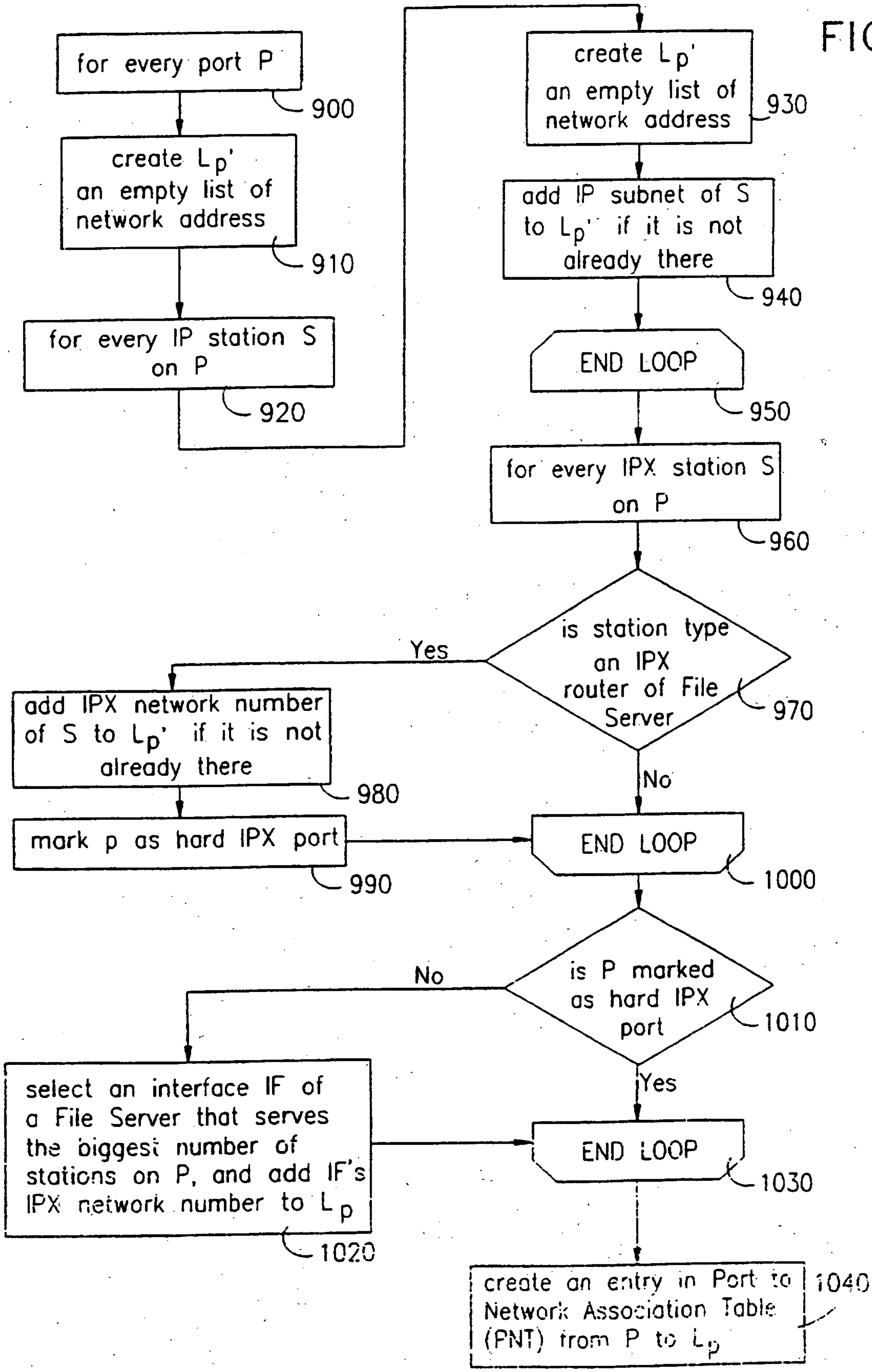
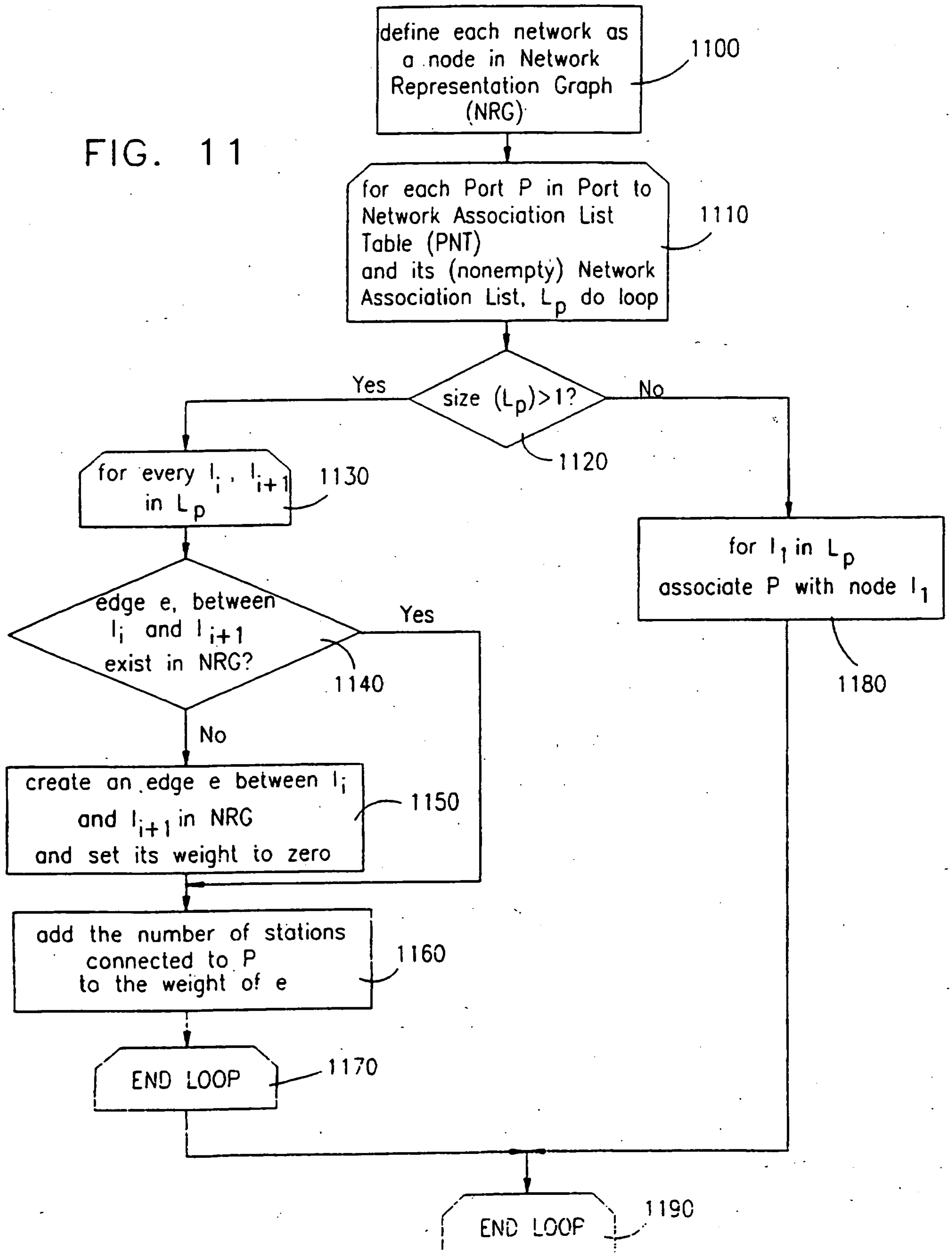

for every port P
900
create Lp' an empty list of network address
910
for every IP station S on P
920
create Lp' an empty list of network address
930
add IP subnet of S to Lp'' if it is not already there
940
END LOOP
950
for every IPX station S on P
960
is station type an IPX router of File Server
970
Yes
No
add IPX network number of S to Lp' if it is not already there
980
mark p as hard IPX port
990
END LOOP
1000
is P marked as hard IPX port
1010
No
Yes
select an interface IF of a File Server that serves the biggest number of stations on P, and add IF's IPX network number to Lp
1020
END LOOP
1030
create an entry in Port to Network Association Table (PNT) from P to Lp
1040

FIG. 11


define each network as a node in Network Representation Graph (NRG)
1100
for each Port P in Port to Network Association List Table (PNT) and its (nonempty) Network Association List, Lp do loop
1110
size (Lp)>1?
1120
Yes
No
for every li , li+1 in Lp
1130
edge e, between li and li+1 exist in NRG?
1140
Yes
No
create an edge e between li and li+1 in NRG and set its weight to zero
1150
add the number of stations connected to P to the weight of e
1160
END LOOP
1170
for l1 in Lp associate P with node l1
1180
END LOOP
1190

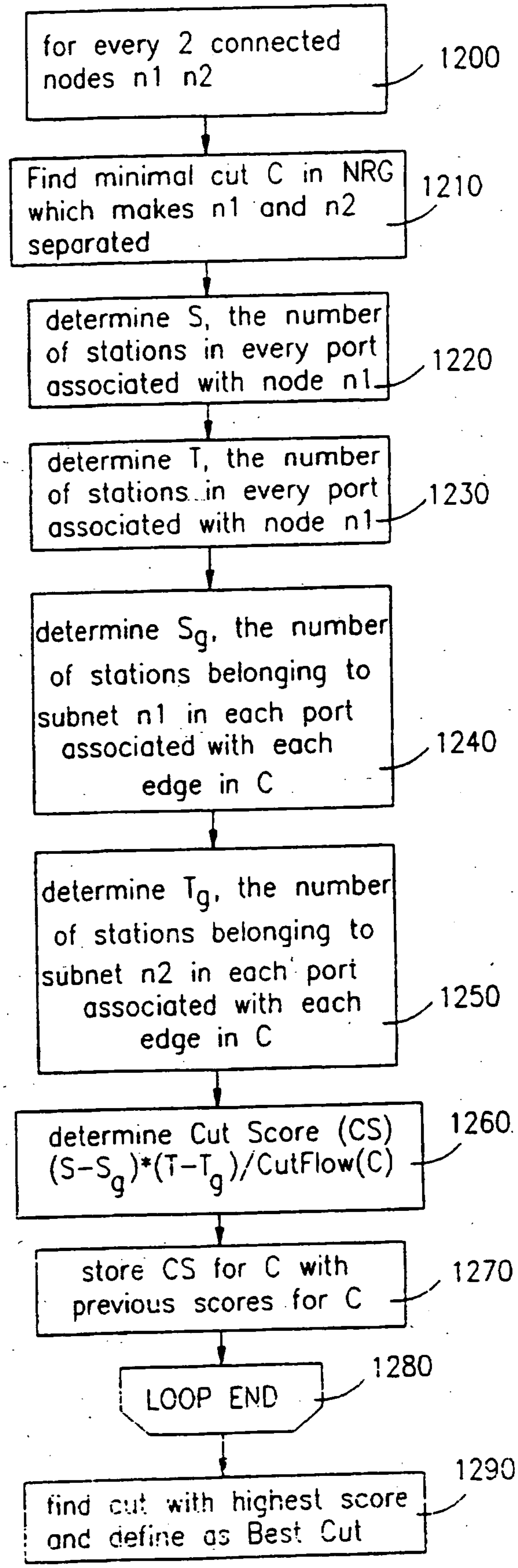

for every 2 connected nodes n1 n2
1200
Find minimal cut C in NRG which makes n1 and n2 separated
1210
determine S, the number of stations in every port associated with node n1
1220
determine T, the number of stations in every port associated with node n1
1230
determine S_g, the number of stations belonging to subnet n1 in each port associated with each edge in C
1240
determine T_g, the number of stations belonging to subnet n2 in each port associated with each edge in C
1250
determine Cut Score (CS) $(S-S_g)*(T-T_g)/CutFlow(C)$
1260
store CS for C with previous scores for C
1270
LOOP END
1280
find cut with highest score and define as Best Cut
1290

FIG. 12

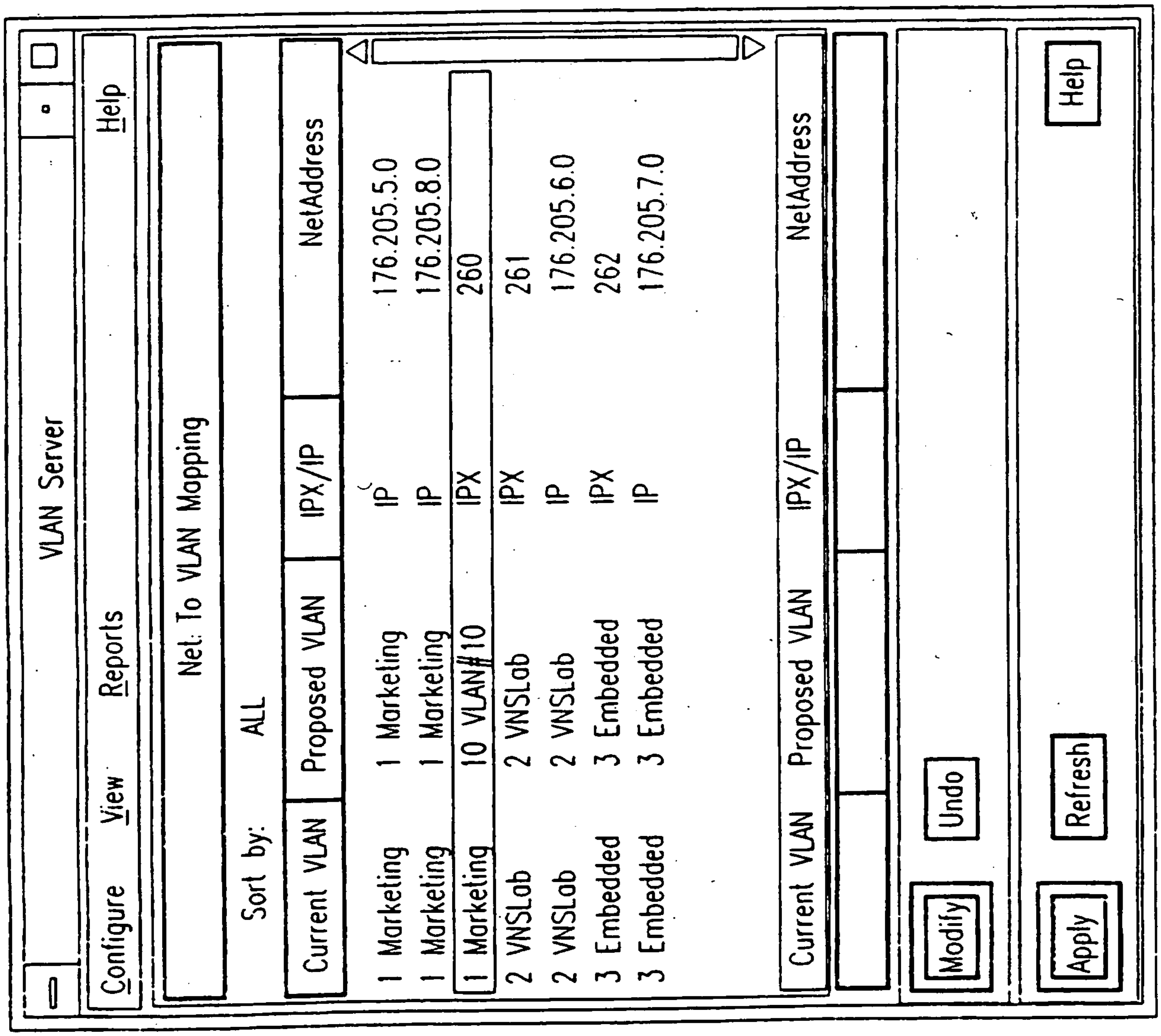
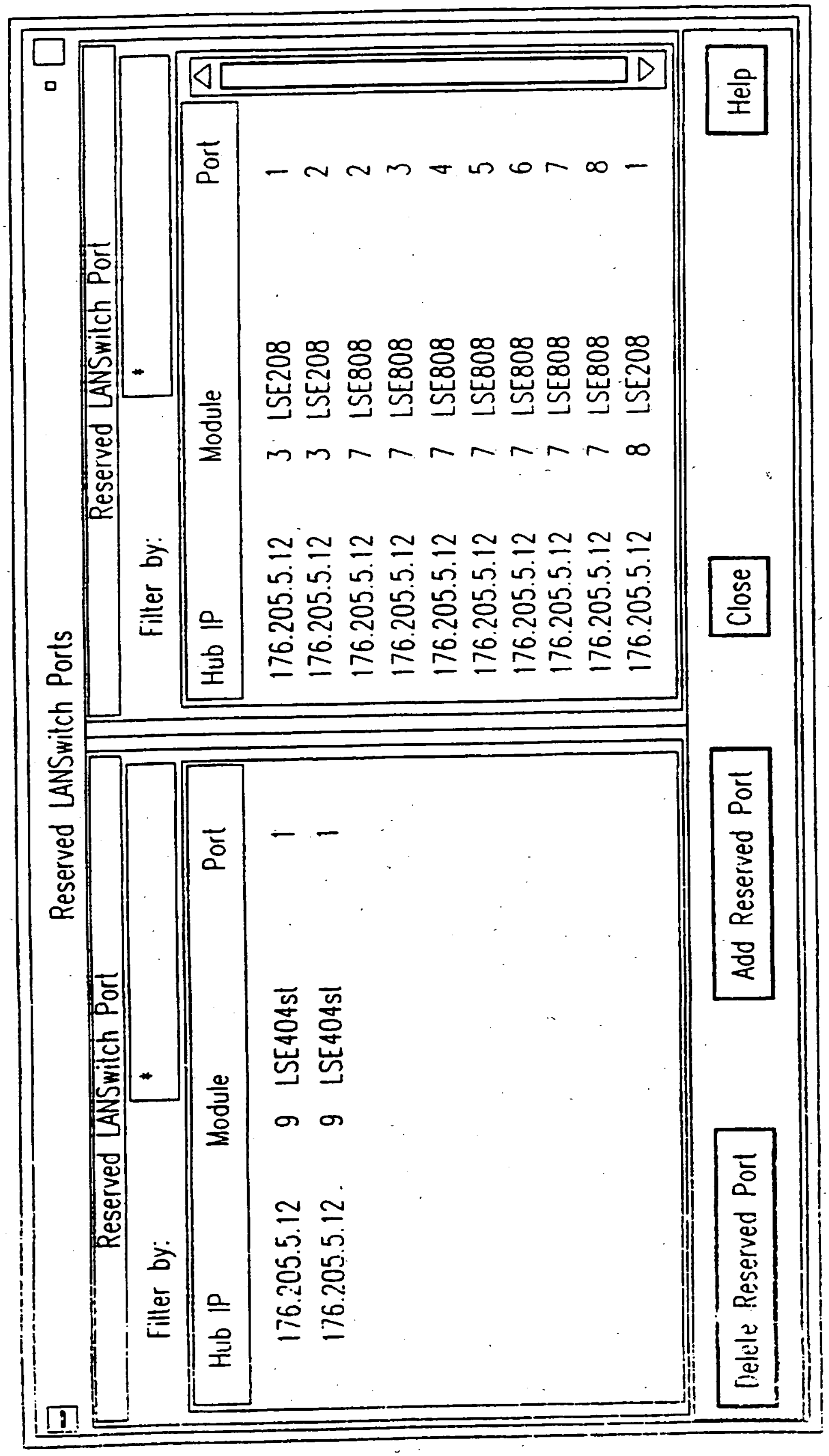

VLAN Server
Configure
View
Reports
Help
Net. To VLAN Mapping
Sort by: ALL
Current VLAN
Proposed VLAN
IPX/IP
NetAddress
1 Marketing
1 Marketing
IP
176.205.5.0
1 Marketing
1 Marketing
IP
176.205.8.0
1 Marketing
10 VLAN#10
IPX
260
2 VNSLab
2 VNSLab
IPX
261
2 VNSLab
2 VNSLab
IP
176.205.6.0
3 Embedded
3 Embedded
IPX
262
3 Embedded
3 Embedded
IP
176.205.7.0
Current VLAN
Proposed VLAN
IPX/IP
NetAddress
Modify
Undo
Apply
Refresh
Help

FIG. 13

FIG. 14


Reserved LANSwitch Ports
Reserved LANSwitch Port
Filter by:
*
Hub IP
Module
Port
176.205.5.12 9 LSE404sl 1
176.205.5.12 9 LSE404sl 1
Reserved LANSwitch Port
Filter by:
*
Hub IP
Module
Port
176.205.5.12 3 LSE208 1
176.205.5.12 3 LSE208 2
176.205.5.12 7 LSE808 2
176.205.5.12 7 LSE808 3
176.205.5.12 7 LSE808 4
176.205.5.12 7 LSE808 5
176.205.5.12 7 LSE808 6
176.205.5.12 7 LSE808 7
176.205.5.12 7 LSE808 8
176.205.5.12 8 LSE208 1
Delete Reserved Port
Add Reserved Port
Close
Help

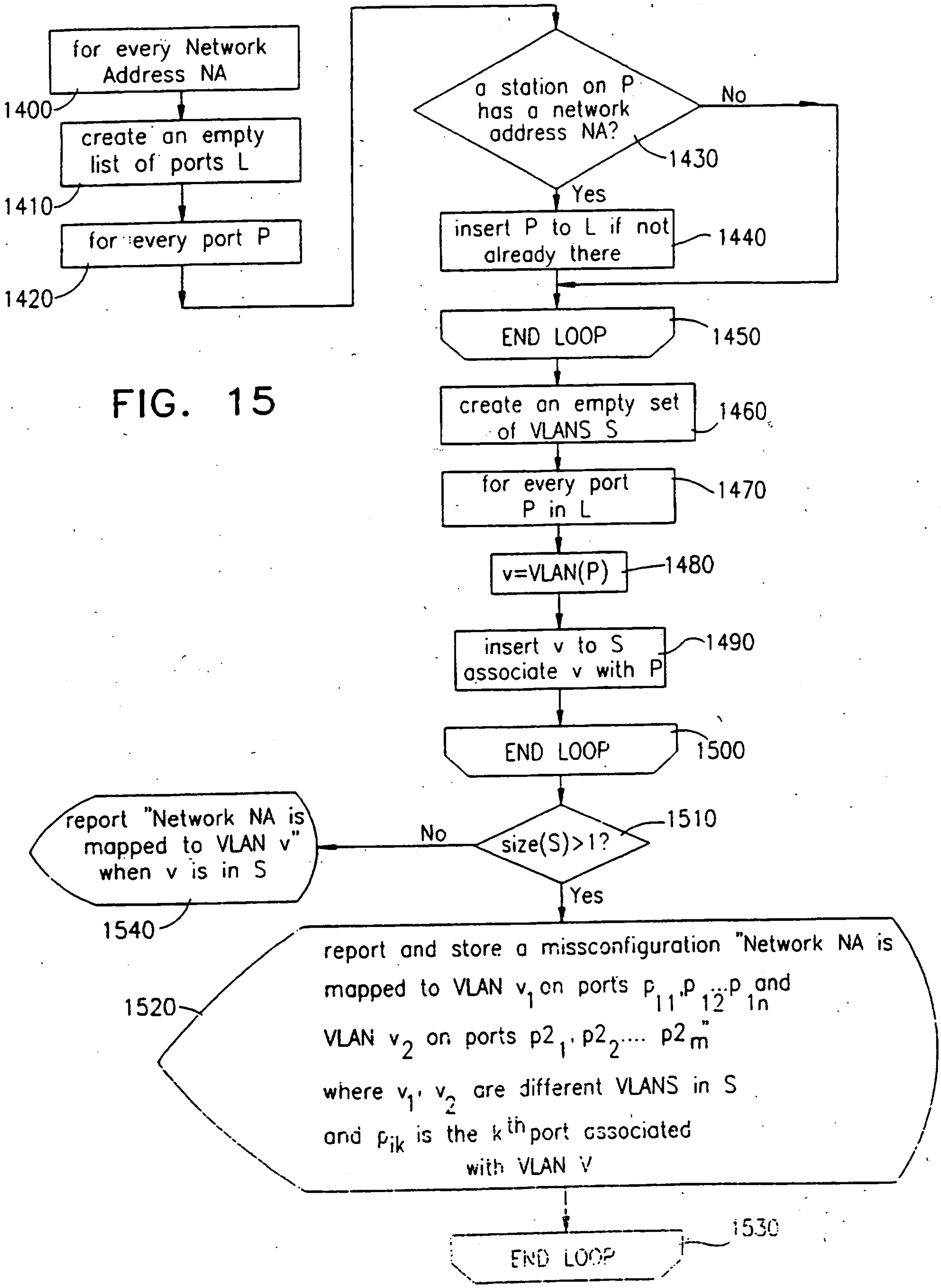

for every Network Address NA
1400
create an empty list of ports L
1410
for every port P
1420
a station on P has a network address NA?
1430
No
Yes
insert P to L if not already there
1440
END LOOP
1450
create an empty set of VLANS S
1460
for every port P in L
1470
v=VLAN(P)
1480
insert v to S associate v with P
1490
END LOOP
1500
size(S)>1?
1510
No
report "Network NA is mapped to VLAN v" when v is in S
1540
Yes
report and store a missconfiguration "Network NA is mapped to VLAN v1 on ports p11,p12...p1n and VLAN v2 on ports p21, p22.... p2m" where v1, v2 are different VLANS in S and pik is the kth port associated with VLAN V
1520
END LOOP
1530

FIG. 15

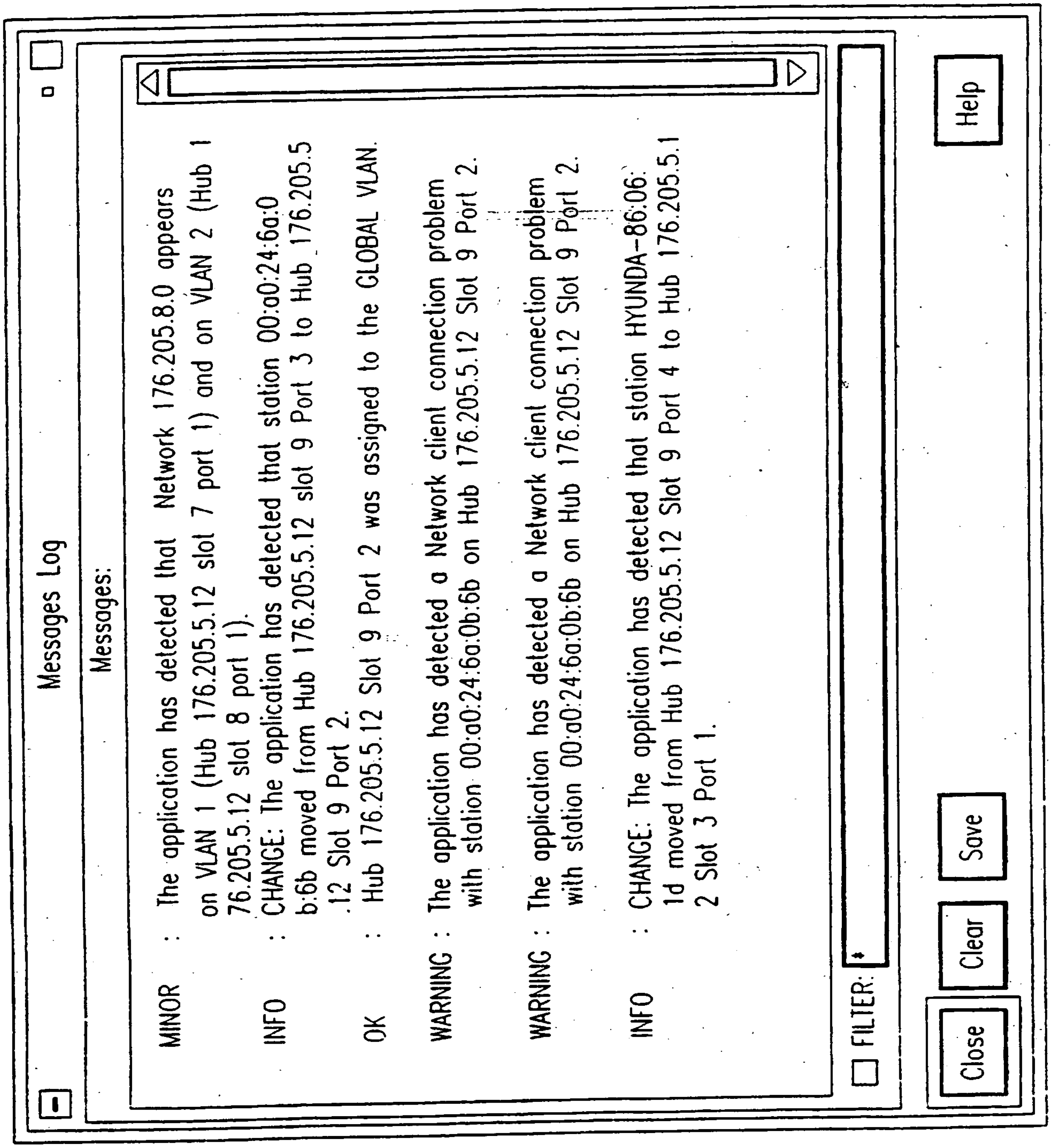

Messages Log
Messages:
MINOR : The application has detected that Network 176.205.8.0 appears on VLAN 1 (Hub 176.205.5.12 slot 7 port 1) and on VLAN 2 (Hub 176.205.5.12 slot 8 port 1).
INFO : CHANGE: The application has detected that station 00:a0:24:6a:0b:6b moved from Hub 176.205.5.12 slot 9 Port 3 to Hub 176.205.5.12 Slot 9 Port 2.
OK : Hub 176.205.5.12 Slot 9 Port 2 was assigned to the GLOBAL VLAN.
WARNING : The application has detected a Network client connection problem with station 00:a0:24:6a:0b:6b on Hub 176.205.5.12 Slot 9 Port 2.
WARNING : The application has detected a Network client connection problem with station 00:a0:24:6a:0b:6b on Hub 176.205.5.12 Slot 9 Port 2.
INFO : CHANGE: The application has detected that station HYUNDA-86:06:1d moved from Hub 176.205.5.12 Slot 9 Port 4 to Hub 176.205.5.12 Slot 3 Port 1.
FILTER:
Close
Clear
Save
Help

FIG. 16

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/46, 12/24

A3

(11) International Publication Number: WO 98/05146

(43) International Publication Date: 5 February 1998 (05.02.98)

(21) International Application Number: PCT/IL97/00258

(22) International Filing Date: 29 July 1997 (29.07.97)

(30) Priority Data:
118984 30 July 1996 (30.07.96) IL

(71) Applicant: MADGE NETWORKS (ISRAEL) LTD. [IL/IL]; Building 3, Atidim Technology Park, 61131 Tel Aviv (IL).

(72) Inventors: BERLOVITCH, Albert; Benyamin Fine Street 4, 75237 Rishon le Zion (IL). SHURMAN, Michael; Greenspan Street 4221, 93806 Jerusalem (IL). SHOUA, Menachem; Hapodim Street 30, 52574 Ramat Gan (IL).

(74) Agents: COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States: CN, JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

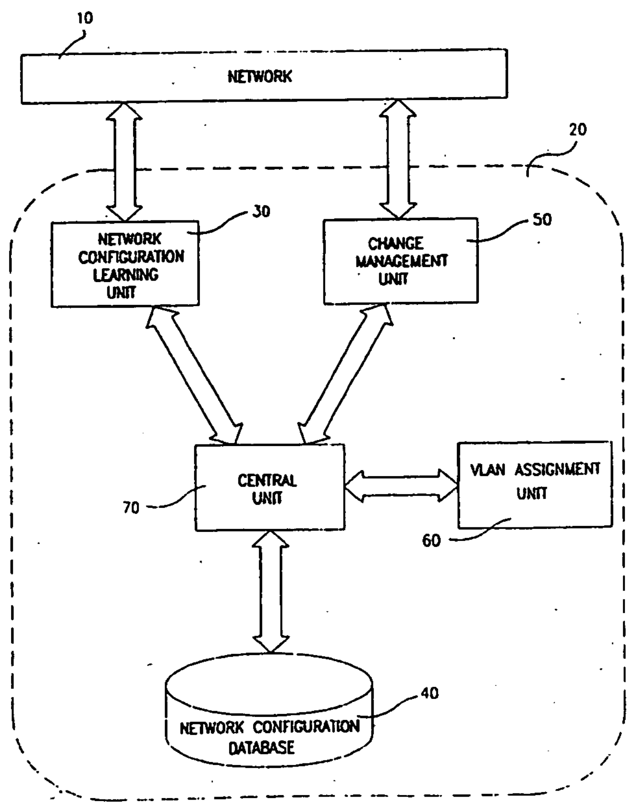
Published
With international search report.

(88) Date of publication of the international search report: 30 April 1998 (30.04.98)

(54) Title: APPARATUS AND METHOD FOR ASSIGNING VIRTUAL LANs

(57) Abstract

This invention discloses an apparatus (20) for managing a switched routed network (10) including a network configuration learning unit (30) operative to learn a configuration of the switched routed network, a VLAN assignment unit (60) for generating a division of the network into virtual LANs (VLANs) based on the learned configuration of the network, and a change manager (50) operative to detect a change in the configuration of the network and to modify the division of the network into VLANs. A method for generating a division of a switched routed network into virtual LANs (VLANs) based on a learned configuration of the network is also disclosed.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 97/00258

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/46 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 13, no. 5, 1 June 1995, pages 839-849, XP000499090 MYLES A ET AL: "A MOBILE HOST PROTOCOL SUPPORTING ROUTE OPTIMIZATION AND AUTHENTICATION" see paragraph 2B-2D see paragraph 5-5B see paragraph 6C see paragraph 8 ---	1,2

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

5

Date of the actual completion of the international search	Date of mailing of the international search report
1 December 1997	25.02.98

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dupuis, H

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 615 362 A (HEWLETT PACKARD CO) 14 September 1994 see column 1, line 43-45 see column 3, line 2 - column 4, line 24 see column 8, line 2 - column 9, line 13 see column 12, line 29 - column 13, line 56 see column 19, line 57 - column 20, line 52 ---	26 27-29
Y A	DATA COMMUNICATIONS, vol. 23, no. 12, 1 September 1994, pages 66-70, 72, 74, 76, 78, 80, XP000462385 "SWITCHED VIRTUAL NETWORKS INTERNETWORKING MOVES BEYOND BRIDGES AND ROUTERS" see page 70, right-hand column, line 53 - page 74, left-hand column, line 5; figures 3,4 see page 76, left-hand column, line 23 - middle column, line 35 -----	27-29 1,26

5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL 97/00258

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see annexed sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1,2,26-29

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

1. Claims 1,2,26-29: An apparatus for managing a switched routed network, comprising a network configuration learning unit, a VLAN assignment unit and a change manager, wherein the network configuration learning unit comprises a diagnostic unit for analysing and diagnosing the existing division of the network into VLANs.

2. CLaims 3-19,25: An apparatus and method for learning the configuration and generating a division into VLAN of a switched routed network, the network comprising at least one switching hub and a plurality of endstations each having a unique physical address and connected to a specific port of a switching hub.

3. CLaims 20-24,30-35: A method for detecting a change in the configuration of a switched routed network comprising: detecting at least one event at an individual network element, and categorizing at least one event as a problematic event or a non-problematic event.

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Interr nal Application No
PCT/IL 97/00258

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0615362 A	14-09-94	JP 6348622 A US 5712981 A	22-12-94 27-01-98